Um Estudo de Correlação de Ataques DRDoS com Fatores Externos Visando Dados de Honeypots

Tiago Heinrich[1], **Newton C. Will**[2], **Rafael R. Obelheiro**[3], **Carlos A. Maziero**[1]

[1] Departamento de Informática
Universidade Federal do Paraná (UFPR)
Curitiba – PR – Brasil

[2]Departamento de Ciência da Computação
Universidade Tecnológica Federal do Paraná (UTFPR)
Dois Vizinhos – PR – Brasil

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

{theinrich,maziero}@inf.ufpr.br, will@utfpr.edu.br,
rafael.obelheiro@udesc.br

Abstract. *In recent years* Distributed Reflection Denial of Service *(DRDoS) attacks make headlines when considering the volume of traffic that attackers manage to generate through reflectors. The attacks exploit different strategies, with the possibility of using many protocols for traffic amplification. Aiming to study the influence of external factors in DRDoS attacks, this work uses data collected by honeypots to identify periods of intense DRDoS attacks and tries to associate external factors to these periods. We investigated 13 countries that concentrate the most attacks in each continent and were able to associate external factors, such as political events and COVID-19, with many periods.*

Resumo. *Nos últimos anos ataques DRDoS viraram notícia, considerando o volume de tráfego que atacantes conseguem gerar através de refletores. Os ataques exploram diferentes estratégias, com a possibilidade de utilizar muitos protocolos para a amplificação do tráfego. Visando estudar a influência de fatores externos em ataques DRDoS, este trabalho utiliza dados coletados por* honeypots *para identificar períodos de intensos ataques DRDoS e tenta associar fatores externos a esses períodos. Ao todo foram investigados 13 países que concentram mais ataques em cada continente, e para diversos períodos foi possível associar fatores externos, como eventos políticos e COVID-19.*

1. Introdução

Ataques distribuídos de negação de serviço baseados em reflexão (*Distributed Reflection Denial of Service*, DRDoS) são uma variação dos ataques *Distributed Denial of Service* (DDoS) que explora refletores como meio intermediário para efetuar os ataques. Estes refletores são responsáveis por amplificar o tráfego de ataque, além de garantir mais uma camada de anonimato para o atacante [Paxson 2001]. Os atacantes exploram protocolos Internet que geram respostas maiores dos que as requisições correspondentes. Esses

protocolos, em sua grande maioria, utilizam o *User Datagram Protocol* (UDP), o que permite que os atacantes forjem o endereço de origem das requisições (via IP *spoofing*) de modo que as respostas sejam enviadas para vítimas à sua escolha, e não para a real procedência das requisições. Atualmente, um leque variado de protocolos com diferentes fatores de amplificação pode ser utilizado para esta finalidade, o que acaba colaborando com este tipo de ataque [Rossow 2014, Heinrich and Obelheiro 2019].

Na última década é possível observar um crescimento na presença destes ataques na Internet [Heinrich et al. 2021] e a constante descoberta de novos recursos que podem ser explorados para realizar a amplificação do tráfego [NETSCOUT and Arbor 2017]. Os ataques vêm crescendo não apenas em número mas também em volume, e este fator ainda é combinado com novas estratégias de realização de ataques [Kührer et al. 2014, Krämer et al. 2015, Thomas et al. 2017]. Estes fatores ajudam a explicar a persistência de ataques DRDoS na Internet.

A literatura registra estudos teóricos e empíricos de ataques DRDoS considerando tanto um único protocolo [Anagnostopoulos et al. 2013, Fachkha et al. 2015, Rudman and Irwin 2015] quanto múltiplos protocolos [Rossow 2014, Noroozian et al. 2016]. Estudos também destacam novas estratégias utilizadas pelos atacantes, como *carpet bombing* [Krämer et al. 2015, Heinrich et al. 2021].

Dados coletados por *honeypots* permitem observar diversos aspectos de ataques DRDoS [Thomas et al. 2017, Heinrich and Obelheiro 2019]. O estudo de vítimas e influência de fatores externos em ataques, porém, ainda é incipiente [Heinrich et al. 2021, Kopp et al. 2021]. Visando preencher esta lacuna na literatura, este trabalho explora a influência de fatores externos em ataques DRDoS através de dados coletados por *honeypots*. A ideia é identificar períodos com maior incidência de ataques, e investigar eventos de conhecimento notório que possam estar correlacionados com o aumento de ataques.

Os dados abordados no estudo são de um conjunto de *honeypots* que iniciou a coleta de dados em 2018, alcançando 3 anos e 7 meses de coleta. Ao todo são investigados os 13 países, de seis continentes, com maior incidência de ataques observados pelos *honeypots*. Através deste conjunto de dados visamos:

- Compreender como ataques DRDoS em cada país;
- Estudar a influência de fatores externos em ataques DRDoS; e
- Comparar comportamentos encontrados em diferentes países.

Este trabalho está estruturado em cinco seções. Na Seção 2 são apresentados os trabalhos relacionados. A Seção 3 apresenta o *honeypot* utilizado, estratégia de coleta de dados, avaliação dos dados e discussão de resultados. Por fim, a Seção 4 apresenta a conclusão do trabalho.

2. Trabalhos Relacionados

Diversos trabalhos na literatura exploram e analisam ataques DRDoS, buscando identificar as características e compreender os impactos causados por tais ataques.

Uma análise do tráfego DNS (*Domain Name System*) é conduzida por [Heinrich et al. 2017], destacando o alto fator de amplificação oferecido pelo protocolo DNS e a existência de domínios projetados para amplificação. [Rossow 2014] faz um

levantamento dos protocolos UDP utilizados em diversos serviços de rede, identificando 14 protocolos que podem ser utilizados para amplificação e destacando que outros protocolos são vulneráveis, e não somente o DNS. [Heinrich and Obelheiro 2019] fazem uma análise dos ataques DRDoS no contexto brasileiro, comparando-os com as características dos ataques ao redor do mundo. Os autores descrevem que os ataques efetuados em território brasileiro são menos intensos e sofisticados do que aqueles praticados em outros países, destacando que o cenário nacional pode ter uma piora à medida que os atacantes passem a utilizar os protocolos e técnicas já empregadas ao redor do globo.

[Heinrich and Obelheiro 2019] e [Heinrich et al. 2021] também descrevem a técnica de *carpet bombing*, que consiste em direcionar o tráfego para múltiplos endereços IP em uma mesma sub-rede, com o objetivo de saturar os enlaces de acesso e dificultar a detecção e mitigação do ataque. [Heinrich et al. 2021] destaca que os protocolos já amplamente conhecidos para ataques de amplificação, como *Network Time Protocol* (NTP) e *Domain Name System* (DNS), ainda respondem pela maioria dos ataques, mas que novos protocolos, como *Connectionless Lightweight Directory Access Protocol* (CLDAP), já apresentam um aumento significativo, o que também é observado por [Kopp et al. 2021].

[Ercan and Selçuk 2021] conduziram um levantamento em servidores de 41 países europeus, demonstrando que, enquanto alguns países do continente estão preparados para lidar com ataques DRDoS, outros carecem de estrutura para detectar e mitigar tais ataques.

Diante disso, é importante analisar as características dos ataques geograficamente, para identificar quais são as técnicas e protocolos utilizados em cada região e antecipar possíveis comportamentos dos atacantes, visando implantar técnicas de mitigação em tempo hábil.

3. Análise de Dados

Esta seção apresenta a análise de dados, descrevendo o processo de coleta na Seção 3.1, a avaliação dos dados na Seção 3.2, a distribuição dos ataques DRDoS observados na Seção 3.3, a investigação de fatores externos na Seção 3.4 e a discussão dos resultados na Seção 3.5.

3.1. Coleta de dados

Para a coleta de dados foi usado o MP-H, um *honeypot* voltado para a observação de ataques DRDoS [Heinrich et al. 2021]. O MP-H tem suporte a 9 protocolos: CHARGEN, CLDAP, CoAP, DNS, Memcached, NTP, QOTD, SSDP e Steam. A primeira instância do MP-H iniciou a coleta de dados em setembro de 2018, e com o tempo foram adicionadas mais três instâncias. Esta avaliação considera o conjunto de dados coletados até 28/04/2022, representando um total de 3 anos e 7 meses (1.312 dias).

3.2. Estratégia de avaliação

Para realizar a avaliação, os dados coletados pelos *honeypots* foram processados para identificar os ataques. Devido à semelhança entre os conjuntos de dados utilizados, foi adotada a mesma definição de ataque proposta em [Heinrich and Obelheiro 2019]:

> 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 ataques DRDoS usam IP *spoofing*, e endereço IP de origem das requisições foi considerado como sendo o das vítimas. Esses endereços foram geolocalizados usando a base da MaxMind[1]. Como esse processo resultou em vítimas em mais de 230 países distintos, e averiguar todo conjunto de dados seria inviável, foi necessário adotar uma estratégia para seleção dos países com maior número de ataques. Foram considerados, em cada continente, os países com pelo menos 10% dos ataques. Este critério permite incluir os países mais relevantes em cada região, mesmo aquelas com menor quantidade de ataques.

A Tabela 1 destaca os países selecionados para a avaliação. A porcentagem depois de cada país representa a fração de ataques recebidos por vítimas no país em relação ao total do continente. A América Central não está presente pois a base de geolocalização da MaxMind associa endereços nesse continente à América do Norte ou à América do Sul, dependendo do país, e nenhum país centroamericano atingiu o limiar de 10%. A Antártida foi desconsiderada pela baixa quantidade de ataques.

Tabela 1. Países selecionados para a avaliação.

Continente	País – (%)	Ataques	Requisições	Vítimas	Dias com ataques
Ásia	CN – 21,8	170.840	6.963.084.329	123.810	1.244
	HK – 41,4	324.222	11.380.748.865	235.180	1.157
	SG – 17,9	140.407	5.631.857.218	35.277	1.112
África	EG – 15,3	3.452	14.358.371	5.192	462
	ZA – 61,4	13.849	813.195.078	23.320	716
Europa	DE – 13,8	77.162	1.788.698.420	63.328	1.227
	FR – 13,9	77.647	908.958.788	50.687	1.224
	GB – 23,2	129.316	2.504.915.103	89.189	1.233
América do Norte	US – 90,8	1.234.884	23.851.534.148	879.096	1.258
América do Sul	AR – 13,3	10.262	167.415.965	7.914	985
	BR – 65,4	50.433	12.671.780.579	304.979	1.174
Oceania	AU – 87,2	49.177	1.178.600.364	36.331	1.188
	NZ – 11,9	6.715	210.120.064	5.378	942

Ao comparar o número de ataques e vítimas por país, é possível destacar que grande parte dos países possuem um número de ataques e vítimas próximo. Isso significa que a maioria dos ataques observados tem uma única vítima, e poucas vítimas são atacadas múltiplas vezes. Países que desviam desse comportamento são Brasil (BR), Egito (EG) e África do Sul (ZA). Estes países possuem um número maior de vítimas em relação ao número de ataques. Neste caso, são observados ataques onde múltiplas vítimas estão sendo atacadas ao mesmo tempo, como no caso de ataques de *carpet bombing*.

Em relação ao período de observação, somente África do Sul (ZA), Nova Zelândia (NZ), Argentina (AR) e Egito (EG) possuem menos de 1.000 dias com ataques. Conside-

[1] `https://dev.maxmind.com/geoip`

rando que o período de coleta foi de 1.312 dias, pode-se inferir que, na maioria dos países analisados, ataques foram registrados quase todos os dias.

3.3. Distribuição de ataques

A Figura 1 apresenta a distribuição empírica do número de ataques DRDoS por dia; cada curva representa um dos países investigados. Para que se possa estabelecer o que representa um dia com um número elevado de ataques, é necessário compreender a distribuição do número diário de ataques.

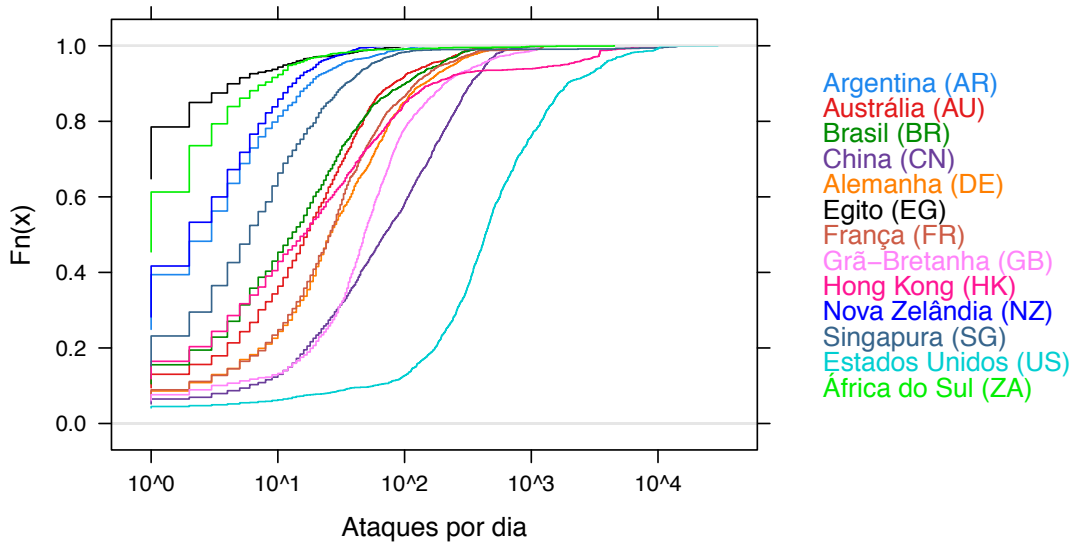

Figura 1. Distribuição empírica de ataques DRDoS por dia (eixo *x* em escala logarítmica).

De modo geral, as distribuições empíricas mostram uma concentração de poucos ataques por dia. Países como AR, EG, NZ e ZA possuem uma média inferior a onze ataques por dia. Na distribuição empírica, estes países têm entre 60% e 80% dos dias com menos de dez ataques.

Este comportamento é similar para os outros países, com diferenças na magnitude dos ataques diários. Países como Austrália (AU) e Brasil (BR) possuem uma média diária de ataques entre 37 e 38, com 3º quartil (Q_3) de 39 e 35, respectivamente. Avaliando as distribuições de ataques diários dos países até este ponto, pode-se afirmar que: (1) em até 75% dos dias foi observado um número pequeno de ataques diários; e (2) apesar de diferentes magnitudes, os comportamentos são similares entre os países.

China (CN), Alemanha (DE), França (FR), Grã-Bretanha (GB) e Singapura (SG) possuem um número médio de ataques por dia entre 58 e 107. Estes países possuem um Q_3 próximo da respectiva média de ataques diários. As observações possuem um comportamento similar aos países anteriores, exceto que os 25% dos dias com mais ataques observados destacam-se em relação ao resto da distribuição (isto é, a distribuição empírica começa a exibir uma cauda mais alongada).

Hong Kong (HK) e Estados Unidos (US) reforçam este achado, sendo possível observar com clareza na distribuição empírica uma cauda alongada nos 15–20% dos maiores valores da distribuição. Ao considerar os 25% dos dias com mais ataques observa-se um

Q_3 de 57 e 940, e um 95-percentil de 1.779 e 3.719, respectivamente. Este crescimento é similar em outros países, embora com diferentes magnitudes.

Analisando todos os países considerados, é possível afirmar que em 75% dos dias o número de ataques observados é parecido e relativamente baixo, e que nos 25% de dias restantes o número de ataques é consideravelmente maior. A hipótese que se pretende investigar é se é possível associar os dias com maior número de ataques a eventos externos. Para verificar essa hipótese, definiu-se que, para um dado país, os dias de interesse são aqueles em que o número de ataques é superior ao Q_3 do país.

3.4. Fatores externos

Fatores externos observados não seguem a mesma distribuição de ataques diários esperados. Como apresentado na Seção 3.3, estes ataques estão presentes em períodos específicos, e são identificados devido à distorção no número de ataques diários. Visando o estudo de fatores externos, a Tabela 2 exibe estatísticas (média, 3º quartil e alguns percentis superiores) sobre o número de ataques observados por dia, assim como o crescimento anual média observado por país. Os casos em que a média é superior ao Q_3 representam caudas longas à direita, com um número pequeno de dias tendo um volume de ataques significativamente maior. Esses dias correspondem aos períodos para os quais se busca correlacionar eventos externos.

Por fim, é apresentado a média de crescimento anual de ataques DRDoS observado em cada país. No geral, observa-se um crescimento pequeno de ano para ano, com somente cinco países tendo um crescimento superior a 3%. Devido ao tempo de coleta dos *honeypots*, é esperado um crescimento menor em decorrência do longo período de coleta.

Tabela 2. Estatísticas de ataques diários e de crescimento anual de ataques por país.

	AR	AU	BR	CN	DE	EG	FR	GB	HK	NZ	SG	US	ZA
Média	7,8	37,4	38,4	130,2	58,81	2,6	59,18	98,5	247,1	5,1	107	941,2	10,5
Q_3	7	39	35,2	188,2	66	1	54	90	57,2	6	15	940,2	3
P_{80}	10	47	45,8	226	77	2	66	109	76,8	8	20	1.200,4	4
P_{90}	18	91,9	101	335,9	141	4,9	122,8	205	165,9	13	34	1.929,2	8
P_{95}	31,4	156	192,4	436,5	243,9	12	200,9	400,7	1.779,2	20	54	3.719,7	13
P_{99}	97,1	326,7	354,9	666,6	492,9	56,6	1.066	1.085	4.339,3	40,8	187,8	9.473,2	59,4
crescimento anual médio (%)	2,8	0,7	3,7	0,9	2,1	11,7	3,2	1,3	3,5	0,4	6,7	1,8	1,1

As seções seguintes apresentam o resultado da investigação para os 13 países considerados. Para cada país, identificou-se os períodos com número superlativo de ataques (de acordo com a definição introduzida na Seção 3.3) e realizou-se uma pesquisa por notícias que ajudassem a entender o contexto do que estava acontecendo no país nesses períodos.

3.4.1. Argentina (AR)

Na Argentina (AR), os períodos com número exacerbado de ataques foram de 21/07 a 09/08/2019 e de 22/01 a 19/02/2021. O primeiro período inicia um mês antes das eleições, sendo que em 2019 foram realizadas eleições provinciais e gerais de forma conjunta

[Liotti 2019]. O diferencial deste ataque está nas vítimas, que estavam espalhadas por diferentes provedores de Internet argentinos. Este foi o primeiro grupo de ataques na AR que não seguia o padrão anterior de ataques. Os ataques ocorreram ao decorrer de 18 dias, e somaram 56,6% dos ataques contra vítimas argentinas observados em 2019. O segundo período corresponde à época em que houve escândalos envolvendo a vacinação da COVID-19 [Rey 2021], onde injustiças na fila de vacinação foram descobertas (pessoas furando a fila). Neste período de 28 dias, observamos 51,3% dos ataques de 2021 na AR, com 514 vítimas distintas.

3.4.2. Austrália (AU)

Na Austrália (AU), o maior aumento no número de ataques no país foi observado em julho de 2019, com um crescimento de 210% em relação ao período anterior. Esse período corresponde à realização do Talisman Saber, um exercício de treinamento militar com os Estados Unidos [AustraliaNaviation 2019]. Outros períodos de crescimento no número de ataques foram observados em agosto e dezembro de 2020, logo após a adoção de restrições e *lockdowns* em certas regiões do país [Saunokonoko 2020, Brown and McMah 2020]. Eventos relacionados à COVID-19 já demonstraram um crescimento no número de ataques como observado em [Heinrich et al. 2021]. Entre 15 e 23/09/2021 foi observado um comportamento similar em relação aos ataques, concomitante com períodos de protestos contra a vacinação obrigatória contra COVID-19 [7News 2021, Seyfort and Zagon 2021]. Entre 07 e 28/04/2022 foram observados 62,4% de todos os ataques de 2022 na AU. O período coincide com a época das campanhas eleitorais no país [Murphy and Butler 2022]. Os ataques foram realizados em 542 vítimas distintas, com uma duração média de 4,8 minutos e média de requisições por ataque de 3.770. Apesar da pequena duração dos ataques, o número de requisições e a concentração destes ataques em um único período demonstra o impacto que um ataque DRDoS pode ter.

Por fim, é interessante apontar a variação nos protocolos utilizados para realizar estes ataques. Apesar de um conjunto variado de protocolo ser utilizados, ataques associados à COVID-19 exploraram DNS e CHARGEN em 95,7% dos ataques observados, já os ataques durante o período eleitoral exploraram o CLDAP em 91,7% dos ataques. Hipóteses que podem explicar essa diferença incluem diferentes entidades efetuando os ataques, ou variação na escolha dos protocolos utilizados para realizar ataques DRDoS em busca de um maior fator de amplificação.

3.4.3. Brasil (BR)

No Brasil (BR) os períodos em que o número de ataques é superior ao Q_3 demonstra a utilização de um ataque em específico. Durante estes períodos foram observados ataques *carpet bombing* contra pequenos provedores de Internet, que geralmente estão isolados em uma única região. O primeiro ocorreu em 11/10/2018, quando foram observados 16 ataques *carpet bombing* a vários blocos da rede de um provedor Internet no Rio de Janeiro. As vítimas foram atacadas durante o horário comercial, totalizando 284 ataques contra 747 vítimas distintas em um único dia. Até junho de 2021 observamos outros 11 ataques de *carpet bombing* com dinâmicas semelhantes. Não foram identificados fatores externos (de notório conhecimento) que pudessem ser associados a esses períodos de ataques, embora saiba-se extraoficialmente que esse tipo de ataque é comum em casos de extorsão contra

pequenos provedores.

3.4.4. China (CN)

A China (CN) teve a quarta maior média de ataques diários. 85,5% dos períodos anormais ficaram concentrados em dois anos, 2019 e 2020. Em 04/01/2019 observamos um pico no número de ataques, explorando o Memcached. Estes ataques ficaram caracterizados pela semelhança no número de requisições enviadas para os *honeypots*, com uma média de 2.406,2 requisições por ataque. Avaliando as vítimas, foi observado que 233 blocos CIDR estavam envolvidos, os quais pertencem a três entidades associadas com telecomunicações. No mês seguinte observou-se um ataque semelhante, que explorou o Memcached como refletor e teve como vítima uma operadora de telecomunicações estatal chinesa. Estes ataques duraram 6 dias, e tiveram o mesmo comportamento em relação ao número de requisições (média de 4.640,4 requisições por ataque). Ao todo, 5.519 ataques foram observados para esta vítima neste período. Este padrão é recorrente em ataques da CN, onde um protocolo específico é associado a um grande número de ataques em um período curto de tempo, com uma média de requisições próxima entre os ataques. Este padrão continua até as observações mais recentes. Em novembro de 2021 observou-se ainda dois períodos com ataques vinculados a estatais chinesas. Não foi possível, no entanto, encontrar eventos externos que pudessem ser associados aos ataques contra vítimas chinesas.

3.4.5. Alemanha (DE)

Na Alemanha (DE) os ataques observados tendem a se estender ao longo de alguns dias, tendo sido observados 303 dias com mais de 200 ataques por dia. Em 19/04/2019 foi presenciado um conjunto de ataques que duraram 5 dias, com 74,8% dos ataques concentrados em quatro *Autonomous System Numbers* (ASNs). Esses ASNs estão vinculados a Amazon e Hetzner, que fornecem serviços de hospedagem. Estes ataques destacam-se pelo volume de requisições, com uma média de 38.963,1 requisições por ataque, e pelo fato dos atacantes terem explorado apenas dois protocolos, CHARGEN e Memcached. Este mesmo conjunto de vítimas reapareceu após três meses em uma nova leva de ataques que durou 18 dias. Já em agosto de 2020 foi observado um crescimento no número de ataques durante protestos contra as medidas adotadas pelo governo para conter a COVID-19, e também foi observado um crescimento no número de ataques durante a tentativa de invasão do parlamento alemão por extremistas [Press 2020]. Na primeira semana de 2021 observou-se um crescimento no número de ataques, bem durante a extensão do prazo de isolamento pela COVID-19 [Beswick 2021].

3.4.6. Egito (EG)

No Egito (EG) são poucos os períodos onde a média diária de ataques possui alguma alteração. Os meses de julho e agosto de 2020 apresentaram 20 dias com um número exacerbado de ataques. Esse período foi imediatamente anterior a protestos populares contra o presidente e militares egípcios, ocorridos em setembro de 2020 [Daragahi 2020].

3.4.7. França (FR)

Na França (FR), foram identificados períodos exacerbados de ataques em março de 2019, justamente em dias que ocorreram protestos contra o presidente [Thomas and Carraud 2019]. Entre 21/07 e 09/08/2019 foram observados ataques com vítimas espalhadas entre a FR, DE e GB. Estes ataques estão divididos em dois períodos, um de 10 e outro de 8 dias, e totalizam 27.850 vítimas distintas. Não foi encontrado nenhum fator concomitante a este ataque que associasse os três países, apesar de parte deste período estar vinculado com fatores apresentados na Seção 3.4.8.

3.4.8. Grã-Bretanha (GB)

Na Grã-Bretanha (GB) foram observadas algumas mudanças durante o período de julho a agosto de 2019, onde houve um crescimento no número de ataques em um período de 19 dias. Isso chamou a atenção porque nesse período a média de ataques foi maior do que em qualquer mês anterior. Em relação à média dos dois meses anteriores, observou-se um crescimento de 2.411,2%. Esse período foi marcado por instabilidade política, incluindo a renúncia da primeira-ministra Theresa May (anunciada em 24/05) e a votação que escolheu Boris Johnson como novo líder do Partido Conservador (entre 6 e 22/07) e, consequentemente, novo primeiro-ministro (Johnson assumiu em 24/07) [Mills 2019]. Após este período, o número de ataques manteve-se próximo à média.

3.4.9. Hong Kong (HK)

Em Hong Kong (HK) foi observado um dos maiores crescimentos no número de ataques de um ano para o outro em um país, com um aumento de 15,6% em 2021. Este foi o país com a segunda maior média de ataques diários, ficando só atrás dos Estados Unidos (US). O diferencial dos ataques observados em HK é a duração, com muitos ataques durando vários dias. Ao todo, em 6% dos dias foram observados mais de 1.000 ataques em um único dia, com um pico de 16.193 ataques. Este volume de ataques ficou concentrado em quatro meses de 2021 (que representa 4,8% dos dias), período em que ocorreram mudanças na legislação relacionadas a telecomunicações e eleições [GovHK 2021, Press 2019].

3.4.10. Nova Zelândia (NZ)

Na Nova Zelândia (NZ) observou-se a segunda menor média de ataques diários, bem como a menor média de crescimento no número de ataques DRDoS por ano. Os períodos que apresentam alteração no comportamento de ataque em 2019 e 2020 coincidem com eventos políticos como eleições locais e gerais [Stuff 2020, Localcouncils 2019a].

3.4.11. Singapura (SG)

Em Singapura (SG) foram identificados dois períodos com ataques cibernéticos contra o governo, 16 a 18/03/2019 e 04 a 06/06/2019. Os ataques observados em SG tendem a explorar diferentes estratégias nos ataques DRDoS. Em um único dia foi possível observar inúmeros ataques DRDoS para vítimas em diferentes redes (estas vítimas não aparentam estar vinculadas) e um ataque *carpet bombing* distribuído em 6 blocos CIDR. Enquanto os ataques DRDoS observados apresentam um volume variado, com as vítimas

recebendo entre 219 e 40.268 requisições por ataque, o ataque *carpet bombing* enviava apenas 112 requisições por vítima. Este volume parece pequeno ao considerar os ataques anteriores, mas é importante ressaltar que até 87 vítimas por bloco CIDR recebiam estas requisições amplificadas, e que o ataque pode ter usado concomitantemente vários outros refletores para direcionar mais tráfego para as mesmas vítimas, com o intuito de dificultar a detecção e a mitigação devido ao grande número de fontes de tráfego, cada uma com uma pequena contribuição individual.

Em dezembro de 2021 e janeiro de 2022 observou-se os períodos com o maior número de ataques por dia, durante onze dias observamos uma média de 14.953 ataques diários. Estes ataques visavam um conjunto de endereços de uma empresa especializada em hospedagem. Ao todo 51.076 vítimas distintas foram atacadas neste período, com todos os endereços pertencendo a esta empresa.

Não foram identificados fatores externos que podessem ser associados aos períodos de ataques exacerbados em SG.

3.4.12. Estados Unidos (US)

Nos Estados Unidos (US), houve um crescimento de ataques durante um curto período de dias no início de 2021. No dia 6 de janeiro, foi observado um crescimento de 44,4% em relação aos dias anteriores; esse crescimento continuou até o dia 11, quando foi observada uma queda de 45,1% no número de ataques (quando as observações voltaram a ficar próximas à média). Comparando o número de ataques observados neste período com o observado em 2020, o crescimento foi de 2.301,2%. Comparando o total de ataques do mês, observa-se um crescimento semelhante no número de ataques de 1.864,6%. Esse período corresponde à invasão do Capitólio na capital Washington, ocorrido em 06/01 [Griffin 2021].

3.4.13. África do Sul (ZA)

Na África do Sul (ZA) foram observados três períodos com número superlativo de ataques: 09 e 10/02/2021, 22 e 23/11/2021, e 26 a 29/01/2022. Estes ataques duraram entre 1 e 3 dias, e se caracterizam como ataques *carpet bombing*. Nota-se o tráfego distribuído entre 58 e 124 blocos CIDR distintos, com um conjunto variado de vítimas por bloco. A única informação adicional encontrada sobre estas vítimas é que elas pertencem a uma mesma plataforma de *hosting* da região. Com relação a fatores externos, nestes períodos pode-se listar problemas políticos e de saúde na região dos ataques [HeraldLIVE 2021, Localcouncils 2019b].

3.5. Discussão

Dentre os 13 países estudados, foram observadas diferentes tendências de acordo com fatores externos. Estes padrões podem estar associados à proximidade física de alguns países ou até mesmo a uma proximidade política. No geral, os ataques e vítimas observados podem destacar certos comportamentos em cada região.

No geral, dois tipos de ataques DRDoS foram observados neste conjunto de dados. O primeiro consiste de ataques DRDoS contra uma única vítima, similar ao padrão observado em ataques DDoS. Já o segundo tipo consiste em uma variação de ataques DRDoS

conhecida como *carpet bombing*. Estes ataques visam a distribuir o tráfego amplificado para um conjunto de vítimas, em vez de concentrar todo o tráfego em uma única vítima. A vantagem desta estratégia está na dificuldade de detecção e mitigação dos ataques, que exige a capacidade de identificar tráfego de ataque de menor intensidade vindo de um número maior de origens e bloquear esse tráfego.

Ao avaliar os países individualmente, foi constatado que, durante os períodos com o maior volume de ataques, é recorrente a presença de múltiplas vítimas em um único bloco CIDR. Considerando todo o conjunto de dados dos 13 países avaliados, somente 5,5% dos ataques observados por dia têm mais de 3 vítimas por CIDR, e somente 0,8% dos ataques têm mais de 20 vítimas por CIDR no mesmo dia. Considerando só os dias com o maior concentração de ataques, estes valores mudam para 4,1% com mais de 3 vítimas por CIDR e 2,5% com mais de 20 vítimas por CIDR. Apesar da divisão do conjunto de dados, o comportamento aparenta ser similar entre os dois formatos de ataque observados.

O crescimento anual de ataques foi, no geral, pequeno durante o período em que os *honeypots* realizaram coleta, ficando entre 0,7 e 11,6%. É importante ressaltar que a média anual mascara algumas variações notáveis, como os crescimentos verificados em 2021 para SG (15,5%) e HK (15,6%), os quais foram discutidos na Seção 3.4.

A política destacou-se como um fator externo importante no contexto de ataques DRDoS. Vários períodos com maior incidência de ataques puderam ser associados a diversos fatores políticos, como eleições, reformas legislativas e protestos contra o governo.

Outro fator externo que pode ser relacionado a alguns dos ataques observados foi a COVID-19. Na literatura já é apontado um crescimento de ataques devido às condições do *lockdown* causadas pela COVID-19 [NETSCOUT 2020]. Os 13 países estudados refletem este comportamento, com períodos de *lockdown* ou aplicação de medidas restritivas, correspondendo a um crescimento no número de ataques DRDoS.

Uma questão que pode ser levantada é se as associações entre ataques e fatores externos apontadas neste artigo são suficientes para estabelecer um nexo de causalidade ou apenas uma correlação. Em grande medida, essa questão é, na verdade, irrelevante. Em primeiro lugar, não se pretende aqui estabelecer causalidade entre os fatores externos e os ataques observados, mesmo porque os dados disponíveis não são suficientes para tal inferência. Em segundo lugar, a correlação entre os eventos é o bastante para que organizações possam, por exemplo, tomar medidas adicionais de precaução (como contratar ou incrementar serviços anti-DDoS) em períodos de volatilidade política.

Uma limitação do presente estudo é a eventual inexatidão dos dados de geolocalização. O grande número de vítimas inviabiliza qualquer tentativa de verificar manualmente a exatidão das localizações indicadas pela base da MaxMind. Um caso particularmente sensível é o de redes de distribuição de conteúdo, provedores de *hosting* e de nuvem, cujos endereços IP podem estar geolocalizados na matriz ainda que na prática estejam em (ou hospedem conteúdos de) outras regiões. Esta limitação é difícil de ser contornada na medida em que o tráfego de ataque, coletado por *honeypots* recrutados para atuarem como refletores em ataques DRDoS, não contém nenhuma identificação do alvo visado. Por outro lado, caso ataques contra vítimas em um país sejam indevidamente contabilizadas em outro país, a consequência mais provável para este estudo é impedir a associação de fatores externos aos períodos de tais ataques, uma vez que tais fatores não

serão encontrados ao serem procurados no país incorreto. As associações estabelecidas, por outro lado, têm menor probabilidade de serem afetadas.

Uma segunda limitação do estudo é a indisponibilidade de informações que permitam associar fatores externos aos ataques observados. Alguns dos países para os quais não foi possível estabelecer nenhuma associação, como China (CN), Egito (EG), Hong Kong (HK) e Singapura (SG), não apenas impõem maiores restrições à circulação de informações, mas também dispõem de menores volumes de informação em idiomas acessíveis aos autores (como português, inglês, espanhol, italiano ou francês). Novamente, o impacto dessa limitação é uma possível subestimativa das associações entre ataques e fatores externos, sem prejuízo das associações já estabelecidas.

4. Conclusão

Ataques DRDoS podem ser estudados através de dados coletados por *honeypots* que forjam vulnerabilidades de serviços que possam ser realizados para a reflexão de tráfego. Na literatura existe um foco em estratégias e tipos de ataques com pouca investigação ao considerar a motivação e influência por trás de ataques DRDoS.

Para realizar este estudo o conjunto de dados foi dividido em 13 países com o maior número de ataques por continente. Estes países apresentaram poucos dias com um número elevado de ataques. Foram identificados esses períodos com número de ataques diários acima do normal, e buscou-se fatores externos que pudessem ser associados a esses períodos, destacando-se fatores políticos e relacionados à COVID-19.

Uma possível extensão deste trabalho seria, em tempo real, identificar períodos com aumento significativo no número de ataques e levantar maiores informações sobre as vítimas envolvidas, especialmente dados voláteis (por exemplo, que *websites* estão hospedados em um endereço pertencente a um provedor de *hosting*).

Agradecimentos

Este trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES), UDESC e FAPESC. Os autores também agradecem o Programa de Pós-Graduação em Informática da UFPR e a UTFPR *Campus* Dois Vizinhos.

Referências

7News (2021). Snap two-week shutdown of construction industry confirmed after violent Melbourne protest. `https://bit.ly/3xAhKYx`.

Anagnostopoulos, M., Kambourakis, G., Kopanos, P., Louloudakis, G., and Gritzalis, S. (2013). DNS amplification attack revisited. *Computers & Security*, 39:475–485.

AustraliaNaviation (2019). Exercise talisman sabre formally launched on USS Reagan. `https://bit.ly/3n0bHYo`.

Beswick, E. (2021). Germany extends and tightens lockdown restrictions to January 31. `https://bit.ly/3bfjYFv`.

Brown, N. and McMah, L. (2020). NSW What northern beaches outbreak means for Christmas borders. `https://bit.ly/3Ol9hjn`.

Daragahi, B. (2020). Riot police crack down on spontaneous demonstrations against President Sisi in cities across Egypt. https://bit.ly/3xFgoM6.

Ercan, E. M. and Selçuk, A. A. (2021). A study on exploitable DRDoS amplifiers in Europe. *International Journal of Information Security Science*, 10(2):26–41.

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

GovHK (2021). New telecoms law to take effect. https://bit.ly/3n1fwNa.

Griffin, D. (2021). Assault on democracy paths to insurrection. https://cnn.it/3NfcNug.

Heinrich, T., Longo, F., and Obelheiro, R. R. (2017). Experiências com um honeypot DNS: Caracterização e evolução do tráfego malicioso. In *Anais do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 292–305, Brasília, DF, Brasil. SBC.

Heinrich, T. and Obelheiro, R. R. (2019). Brasil vs Mundo: Uma análise comparativa de ataques DDoS por reflexão. In *Anais do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 239–252, São Paulo, SP, Brasil. SBC.

Heinrich, T., Obelheiro, R. R., and Maziero, C. A. (2021). New kids on the DRDoS block: Characterizing multiprotocol and carpet bombing attacks. In *Proceedings of the 22nd International Conference on Passive and Active Network Measurement*, pages 269–283, Cottbus, Alemanha. Springer.

HeraldLIVE (2021). It is official, Port Elizabeth has a new name - Gqeberha. https://bit.ly/3N2Xjt5.

Kopp, D., Dietzel, C., and Hohlfeld, O. (2021). DDoS never dies? An IXP perspective on DDoS amplification attacks. In *Proceedings of the 22nd International Conference on Passive and Active Network Measurement*, pages 284–301, Cottbus, Alemanha. Springer.

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 *Proceedings of the 18th International Symposium on Research in Attacks, Intrusions, and Defenses*, pages 615–636, Kyoto, Japão. Springer.

Kührer, M., Hupperich, T., Rossow, C., and Holz, T. (2014). Exit from hell? Reducing the impact of amplification DDoS attacks. In *Proceedings of the USENIX Security Symposium*, San Diego, CA, EUA. USENIX.

Liotti, J. (2019). Vidal decidio que no adelantara las elecciones en Buenos Aires. https://bit.ly/2GaFPMK.

Localcouncils (2019a). About your 2019 local elections. https://bit.ly/3zLoQMA.

Localcouncils (2019b). About your 2019 local elections. https://bit.ly/39yfw3U.

Mills, J. (2019). New prime minister will be announced on july 23. https://bit.ly/3HLz8hJ.

Murphy, K. and Butler, J. (2022). Anthony Albanese commits to anti-corruption watchdog by end of 2022, if Labor wins election. https://bit.ly/3O3HrrB.

NETSCOUT (2020). Netscout threat intelligence report for the first half of 2020. https://bit.ly/3mh3Tzb.

NETSCOUT and Arbor (2017). Insight into the global threat landscape. Netscout Arbor's 13th Annual Worldwide Infrastructure Security Report.

Noroozian, A., Korczyński, M., Gañan, C., Makita, D., Yoshioka, K., and van Eeten, M. (2016). Who gets the boot? Analyzing victimization by DDoS-as-a-Service. In *Proceedings of the 19th International Symposium on Research in Attacks, Intrusions, and Defenses*, pages 368–389, Paris, França. Springer.

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

Press, A. (2019). Hong Kong's delayed legislative elections set for December. https://bit.ly/3b5gaX7.

Press, A. (2020). Anti-corona extremists try to storm German parliament. https://bit.ly/3N2B0DY.

Rey, D. (2021). Argentine health minister resigns amid vaccine scandal. https://bit.ly/3xxshDU.

Rossow, C. (2014). Amplification hell: Revisiting network protocols for DDoS abuse. In *Proceedings of the Network and Distributed System Security Symposium*, pages 1–15, San Diego, CA, EUA. Internet Society.

Rudman, L. and Irwin, B. (2015). Characterization and analysis of NTP amplification-based DDoS attacks. In *Proceedings of the Information Security for South Africa*, Joanesburgo, África do Sul. IEEE.

Saunokonoko, M. (2020). Shock and awe: Victoria declares state of disaster, six-week Melbourne curfew and stage four restrictions. https://bit.ly/3zIvhA5.

Seyfort, S. and Zagon, C. (2021). More than 200 arrests made on third day of Melbourne protests. https://bit.ly/3tLUbLc.

Stuff (2020). Jacinda Ardern delays election to October 17 amid coronavirus outbreak. https://bit.ly/3xDglAv.

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

Thomas, L. and Carraud, S. (2019). French violence flares as yellow vest protests enter fourth month. https://reut.rs/3y0p6pO.