UNIVERSIDADE DO ESTADO DE SANTA CATARINA – UDESC
CENTRO DE CIÊNCIAS TECNOLÓGICAS – CCT
PROGRAMA DE PÓS–GRADUAÇÃO EM COMPUTAÇÃO APLICADA – PPGCA

ANTEPROJETO DE PESQUISA

TEMA: SEGURANÇA, COMPUTAÇÃO PARALELA E DISTRIBUÍDA

CARACTERIZAÇÃO DE ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO POR REFLEXÃO (DRDOS)

RAFAEL TENFEN

JOINVILLE, 2022

RESUMO

Ataques distribuídos de negação de serviço por reflexão (*distributed reflection denial of service*, DRDoS) estão por toda a Internet. Esses ataques apresentam formas eficazes em provocar a indisponibilidade de recursos de rede. Para detectar, mitigar e prevenir ataques DRDoS, é de extrema importância entender como eles funcionam e se caracterizam. Para auxiliar no entendimento de ataques DRDoS, *honeypots* são utilizados para recolher dados que os atacantes enviam para vítimas chamados de *payloads*. Esse projeto de pesquisa tem como objetivo investigar a analisar a evolução dos *payloads* ao longo do tempo e comparar os *payloads* recolhidos entre diferentes *honeypots*.

Palavras-chave: DRDoS. honeypot. Ataque de negação de serviço.

ABSTRACT

Distributed denial of service attacks by reflection (DRDoS) is all over the Internet. These attacks provide effective ways to cause network resources unavailability. To detect, mitigate, and prevent DRDoS attacks, it is extremely important to understand how they work and how they are characterized. Honeypots are used to help understand DRDoS attacks by collecting data from the payload request that the attackers sent to the victims. This research project intends to investigate and analyze the evolution of the payloads over time and also compare the payloads collected by different honeypots.

Keywords: latex. abntex. text editoration.

SUMÁRIO

1	**INTRODUÇÃO**	**4**
1.1	PROPOSTA	**7**
1.2	ESTRUTURA DO DOCUMENTO	**7**
2	**REVISÃO DE LITERATURA**	**8**
2.1	ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO (DDOS)	**8**
2.2	ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO POR REFLEXÃO (DRDOS)	**10**
2.2.1	**Evolução de ataques ao longo do tempo**	**10**
2.2.2	**Principais protocolos utilizados em DRDoS**	**10**
2.3	HONEYPOTS	**12**
2.3.1	**MP-H**	**13**
2.4	TRABALHOS RELACIONADOS	**13**
2.5	CONSIDERAÇÕES DO CAPÍTULO	**15**
3	**PROPOSTA**	**16**
3.1		**16**
4	**ANÁLISE DE DADOS**	**17**
4.1	IMPLANTAÇÃO	**17**
4.2	DEFINIÇÕES ADOTADAS	**17**
4.3	OBSERVAÇÕES GERAIS	**18**
4.4	AVALIAÇÃO POR PROTOCOLO	**19**
4.4.1	**NTP - *Network Time Protocol***	**19**
4.4.2	**DNS - *Domain Name System***	**20**
4.4.3	**Memcached**	**25**
4.4.4	**CoAP**	**26**
4.4.5	**CLDAP**	**27**
4.4.6	**SSDP**	**27**
5	**CONCLUSÃO**	**30**
	REFERÊNCIAS	**31**

1 INTRODUÇÃO

A negação de serviço, ou DoS *(Denial of Service)*, consiste em provocar a indisponibilidade de um recurso computacional, como um serviço, um computador ou uma rede conectada à Internet. Em um ataque de negação de serviço, um atacante com motivação financeira, política ou puramente destrutiva interrompe o serviço de uma vítima adicionando uma carga excessivamente alta de tráfego ao(s) serviço(s) da vítima (ROSSOW, 2014). Servidores possuem recursos computacionais limitados, ao enviar mais requisições do que o dispositivo está preparado para manipular, ocorre o esgotamento de recursos, um modo comum em que o DoS é alcançado (JONKER et al., 2017).

Quando um ataque DoS é realizado pela rede de forma coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado no ataque, recebe o nome de ataque distribuído de negação de serviço (*Distributed Denial of Service*, DDoS). Um ataque DDoS não tem por objetivo direto invadir ou coletar informações, mas sim exaurir recursos e causar indisponibilidade de serviço do alvo (CERT.BR, 2016). Em um ataque distribuído de negação de serviço, o tráfego abusivo chega através de muitos dispositivos diferentes ao mesmo tempo, cada um fazendo uma contribuição relativamente pequena para o ataque (THOMAS; CLAYTON; BERESFORD, 2017).

Ao ser atacado, o alvo de um ataque DDoS não consegue diferenciar os acessos legítimos ao sistema dos maliciosos e pode ficar sobrecarregado ao tentar tratar todas as requisições recebidas (CERT.BR, 2016). Uma maneira comum de iniciar ataques DDoS são *botnets* DDoS, ou seja, redes infectadas por *malware* e computadores remotamente designados para participar dos ataques. Quanto maior a quantidade de agentes em uma *botnet*, maior o seu potencial para exaurir os recursos do alvo, assim como aumenta a dificuldade de distinguir o acesso dos atacantes com os acessos legítimos ao sistema em termos de endereços IP *(Internet Protocol)* (WELZEL; ROSSOW; BOS, 2014).

Os ataques DDoS continuam a se tornar cada vez mais devastadores. Em Agosto de 2021, `Microsoft` registrou e anunciou uma largura de banda de 2.4 Terabits por segundo de ataque distribuído de negação de serviço mitigados contra `Azure Cloud Service`, o maior ataque DDoS até o momento registrado pela companhia (RANGAPUR; KANAKAM; JUBILSON, 2022).

Atacantes podem incrementar seus ataques estruturando-os para utilizarem refletores. Um refletor é qualquer hospedeiro que responde a uma requisição. Assim, por exemplo, todos os servidos Web, DNS e roteadores são refletores (PAXSON, 2001). Refletores podem amplificar a quantidade de dados enviados, ou seja, sua resposta produz mais bytes ou pacotes, ou ambos, do que a requisição recebida. Assim, refletores potencializam o tráfego gerado por um atacante (GONDIM; ALBUQUERQUE; OROZCO, 2020). Esse tipo de ataque é chamado de ataque distribuído de negação de serviço por reflexão (*Distributed*

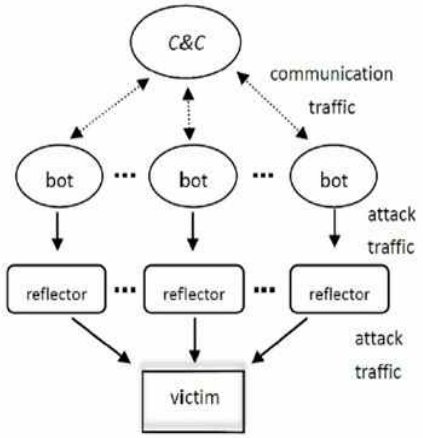
Reflection Denial of Service, DRDoS)

Em um ataque DRDoS o atacante, após infectar outros dispositivos com o *malware* e criar a sua *botnet*, localiza um grande número de refletores, e então orquestra para que os dispositivos infectados iniciem o ataque enviando o tráfego para os refletores, o tráfego enviado contém o endereço de IP de origem da requisição modificado para o endereço de IP da vítima, essa técnica de modificar o endereço de IP é chamada de IP *spoofing*. Dessa forma, os refletores respondem a essas requisições diretamente a vítima.

Os refletores geram tráfego amplificado para a vítima, pois a resposta da requisição dos refletores é de 5,5 até 51.000 vezes (dependendo do protocolo) (HEINRICH, 2019) a quantidade de bytes enviada pelos dispositivos infectados. A vítima por sua vez, não requer nenhum rastreamento para localizar os refletores eles são prontamente identificados como os endereços de origem nos pacotes do ataque recebidos pela vítima. Já o operador de um refletor, não consegue localizar facilmente o dispositivo infectado que está enviando requisições ao refletor, pois o tráfego enviado ao refletor não possui o endereço de origem do dispositivo infectado, mas sim o endereço de origem da vítima (PAXSON, 2001).

Em um ataque DRDoS geralmente são usados servidores de comando e controle C&C *(Command and Control)*, *bots* e refletores na rede, conforme ilustrado na Figura 1.

Figura 1 – Estratégia de ataque distribuído de negação de serviço.



Fonte: (ALIEYAN et al., 2016)

O fluxo apresentado na Figura 1, acontece com o atacante em total poder dos servidores de comando e controle (C&C), que são capazes de instruir os *bots* a enviarem requisições para um ou mais refletores utilizando o endereço de IP do alvo *(victim)* como endereço de origem, levando os refletores infectados a acreditar que a origem das requisições é a vítima, e assim enviar as respostas para essa. Dessa forma, um grande volume de dados chega a vítima pelos refletores sempre que uma conexão com a vítima for estabelecida (ALIEYAN et al., 2016). Portanto, enquanto a vítima estiver sob ataque, ela poderá

sofrer saturação da rede e elevação no consumo de recursos de processamento, memória e armazenamento, com consequente indisponibilidade de serviços.

Nesses ataques utilizando amplificação, um atacante abusa dos chamados dos refletores para esgotar a largura de banda de uma vítima. Um atacante pode abusar de qualquer servidor público vulnerável a ataques de reflexão, como servidores de DNS (Domain Name System) abertos ou servidores NTP (*Network Time Protocol*). Esses protocolos são conhecidos por amplificar significativamente a largura de banda, permitindo facilmente que um atacante lance ataques em escala de Gigabits por segundo com um *uplink* muito menor (KRÄMER et al., 2015).

Uma forma eficiente de observar ataques DRDoS é usando *honeypots*, que são recursos computacionais abertos dedicados a serem sondados, atacados ou comprometidos (HOEPERS; JESSEN; CHAVES, 2007). *Honeypots*, por sua natureza, não são criados para serem acessados por usuários legítimos, e os serviços que eles oferecem não são anunciados. Se a rede de um *honeypot* é monitorado e o *honeypot* é abusado como refletor, é possível associar esse acesso a uma varredura (*scan*) ou ataque DRDoS. Esse é um processo legítimo e natural de detecção de comportamento malicioso (HUSÁK; VIZVÁRY, 2013).

Tendo em vista a relevância dos ataques DRDoS, um foco importante de pesquisa tem sido a análise e caracterização do tráfego associado a esses ataques, com vistas a compreender melhor o seu funcionamento na prática, e assim permitir uma evolução dos mecanismos de defesa. A partir de tráfego DRDoS coletado por um ou mais *honeypots*, são exploradas questões como a duração e a intensidade dos ataques, com que frequência eles ocorrem, quais protocolos são mais usados e quem são as vítimas mais afetadas (HEINRICH, 2019).

Os ataques DRDoS não apenas dificultam a atribuição devido a uma camada extra de indireção, mas também fornecem amplificação de tráfego, facilitando a geração de tráfego suficiente para interromper o alvo, especialmente quando vários refletores são utilizados simultaneamente (HEINRICH; OBELHEIRO; MAZIERO, 2021). Além disso, os ataques DRDoS podem alavancar vários protocolos diferentes, especialmente os baseados em UDP, e há um grande número de servidores de Internet vulneráveis e/ou mal configurados que podem ser usados como refletores (ROSSOW, 2014).

Dois aspectos pouco explorados na literatura dizem respeito aos *payloads* usados em ataques DRDoS. O primeiro é a ausência de uma análise de como esses *payloads* vêm evoluindo ao longo do tempo. O segundo é que trabalhos que usam múltiplos honeypots não comparam os *payloads* entre os honeypots. Pretende-se neste trabalho de mestrado preencher esta lacuna. A pesquisa dá seguimento ao trabalho de (HEINRICH, 2019), e usará os dados de três honeypots, um deles em operação desde 2017 e dois desde 2021.

1.1 PROPOSTA

1.2 ESTRUTURA DO DOCUMENTO

2 REVISÃO DE LITERATURA

Este capítulo faz uma fundamentação dos conceitos necessários ao entendimento deste trabalho baseado na literatura já existente. A Seção 2.2 apresenta fundamentos de ataques DRDoS. A Seção 2.3 aborda conceitos e funcionalidades de *honeypots*. A Seção 2.4 expõe os trabalhos relacionados mais recentes encontrados na literatura.

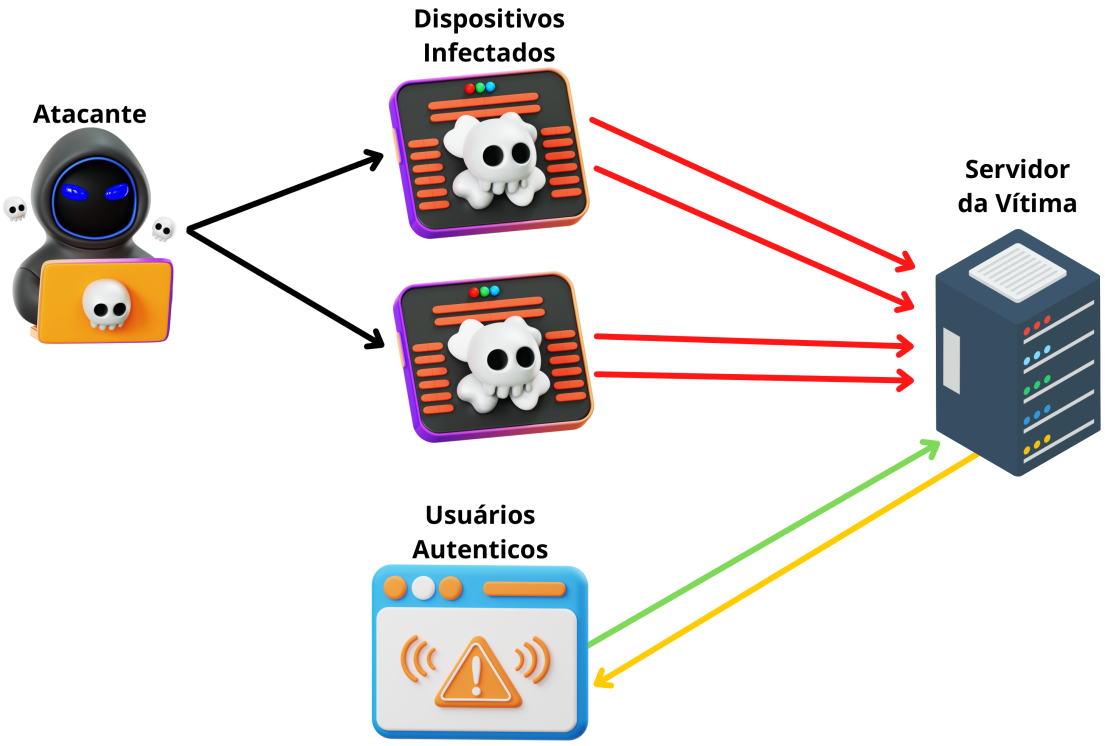
2.1 ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO (DDOS)

A intenção tradicional e o impacto de ataques *Denial of Service* (DoS) são de ~~impedir ou~~ prejudicar o uso legítimo do servidor ou de recursos da rede. Independentemente da diligência, esforço e recursos gastos na proteção contra invasões, os sistemas conectados à Internet enfrentam uma ameaça consistente e real de ataques DoS devido a duas características fundamentais ~~da Internet~~. A primeira é que a internet é composta por recursos limitados e consumíveis que podem ser exauridos. Já, a segunda é que a segurança na internet é altamente interdependente. A interdependência dificulta a padronização e generalização de métodos de segurança, o que intensifica os ataques DoS que são comumente iniciados de um ou mais pontos na Internet que é externa ao próprio sistema ou rede da vítima. Em muitos casos, o ponto de inicialização consiste em um ou mais sistemas que foram infectados por um atacante por meio de um comprometimento relacionado à segurança, e não pelo próprio sistema do atacante (LONG; THOMAS, 2001).

Quando um ataque de negação de serviço é realizado por múltiplas fontes de modo distribuído, é identificado como ataques *Distributed Denial of Service* (DDoS). Conforme apresentado de modo simplificado na Figura 2, um atacante que conseguiu infectar dispositivos com um *malware* que permite o controle desses dispositivos de modo remoto, envia comandos para que os dispositivos infectados enviem tráfego de ataque para uma ou mais vítimas. Além das requisições realizadas pelos dispositivos infectados o servidor da vítima recebe também requisições de seus usuários autênticos e assim, ao receber mais requisições do que consegue processar, o servidor da vítima esgota seus recursos computacionais e não consegue responder a todas as requisições negando serviço aos seus usuários autênticos.

O design da Internet tem seu foco na eficiência de movimentação de pacotes da origem para o destino, esse design segue o paradigma ponta a ponta em que a rede intermediária fornece o serviço de roteamento de pacote com o mínimo de esforço, deixando assim para o cliente e o servidor a implantação de protocolos avançados para obter as garantias de serviço desejadas, como confiabilidade, transporte robusto ou segurança. Esse paradigma empurra a complexidade para os hospedeiros finais, deixando a rede intermediária simples e otimizada para encaminhamento de pacotes. Há uma implicação infeliz, se uma das partes na comunicação bidirecional (cliente ou servidor) se comportar mal, ela pode causar danos

Figura 2 – Ataque DDoS.



Fonte: Autor

arbitrários ao seu par. Nenhum dispositivo na rede intermediária intervirá e impedirá, pois a Internet não foi projetada para policiar o tráfego, uma consequência disso é a presença de IP *spoofing* e a possibilidade de ataques DDoS (MIRKOVIC; REIHER, 2004).

Realizar IP *spoofing* é modificar o endereço IP de um pacote com um endereço falso ou que remete ao endereço de IP de outro dispositivo. Essa técnica emprega uma funcionalidade importante em ataques de negação de serviço pois os atacantes podem se aproveitar para mascarar os ~~seus~~ endereços de origem e dificultar ainda mais a sua identificação. Além de mascarar a sua identidade o IP *spoofing* pode desempenha um outro papel em ataques de negação de serviço, em que o atacante ao invés comandar os dispositivos infectados para enviar requisições para a vítima, enviem requisições para refletores (dispositivos abertos ou mal configurados) na rede e modifiquem o IP de origem da requisição para a vítima, fazendo com que o refletor envie a resposta da requisição para a vítima e assim amplificando o ataque, esse procedimento é identificado como DRDoS.

2.2 ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO POR REFLEXÃO (DRDOS)

Em ataques distribuídos de negação de serviço por reflexão (*distributed reflection denial of service*, DRDoS), um atacante tem como objetivo esgotar a largura de banda da vítima. Ele abusa do fato de que servidores públicos de protocolos de rede baseados em UDP respondem a solicitações sem validar mais a identidade (ou seja, o endereço IP) do remetente (ROSSOW, 2014).

Em um ataque DRDoS, o tráfego recebido pelos refletores tem como origem (forjada) o endereço IP da vítima, fazendo com que o tráfego de resposta seja enviado para esta, e não para os *bots*, como seria de se esperar. É importante destacar que os refletores não são controlados pelo atacante, mas sistemas vulneráveis ou mal configurados que são abusados para a realização de ataques (HEINRICH, 2019).

Os atacantes de ataques DRDoS exploram softwares maliciosos (*malware*) para controlar um grande número de dispositivos na rede (*botnets*) e, em seguida, envia comandos à essas *botnets* para enviar requisições aos amplificadores, falsificando os endereços IP de origem para o usuário alvo (CHEN et al., 2020). Os refletores então ao receberem a requisição com o IP de origem modificado, enviam a requisição de resposta para a vítima.

Ataques DRDoS oferecem aos atacantes vários benefícios, mas os principais são (ROSSOW, 2014):

1. Ele disfarça sua identidade, pois as vítimas recebem tráfego de amplificadores, ou seja, sistemas que podem ser abusados para enviar tráfego para a vítima em nome do atacante;

2. O abuso simultâneo de múltiplos amplificadores permite que um ataque DoS altamente distribuído seja conduzido a partir de um único *uplink* na Internet;

3. O tráfego refletido para a vítima é significativamente maior em largura de banda do que o tráfego que um atacante tem que enviar aos amplificadores.

2.2.1 Evolução de ataques ao longo do tempo

2.2.2 Principais protocolos utilizados em DRDoS

Tabela 1 Linha temporal de ataques de negação de serviço

1974	O primeiro ataque registrado foi realizado explorando uma vulnerabilidade em um mainframe conhecido como *Programmed Logic for Automatic Teaching Operations* (PLATO) (DEAR, 2010).
1988	Robert Morris criou um *malware* conhecido atualmente como *worm*, este foi responsável por paralisar grande parte da Internet (WOODY; MEAD; SHOEMAKER, 2012). Um total de 6000 sistemas UNIX foram infectados para a realização do ataque, por consequência foi a primeira pessoa a ser condenada pela *Computer Fraud and Abuse Act* (CORNELL, 1984).
1995	O Strano Network abria um conjunto elevado de conexões em páginas web como forma de protesto contra a política nuclear do governo francês (COX, 2014).
1997	A primeira demostração pública do ataque DDoS foi realizada por Khan C. Smith, durante o evento grandes corporações acabaram sendo atacadas.
1998	*The Electronic Disturbance Theater* através do FloodNet realizou ataques até o final de 1999, auxiliando protestos no México e realizando ataques em *World Trade Organization* (WTO). Em 1998 também foi realizado o primeiro ataque de reflexão conhecido como *Smurf attacks* que explora o *Internet Control Message Protocol* (ICMP) (RYBA et al., 2015).
1999	Surgimento da *botnet Trinoo* utilizada para a realização de ataques DDoS (LEMOS, 2018). No mesmo ano foi avisado sobre a possibilidade de utilizar o DNS para a realização de ataques DDoS (NIST, 1999; CERT, 1998).
2003	O primeiro *flash worm* (Slammer worm) infectou 75 milhões de *hosts* em dez minutos e alcançou 80 milhões de pacotes por segundo.
2009	O *worm* MyDoom foi reaproveitado para infectar 50 mil *hosts* e realizar um ataque que alcançou picos de 13Gbps (ZETTER, 2009).
2012	Crescimento nos ataques DRDoS explorando DNS, *Character Generator Protocol* (Chargen), NTP e *Simple Network Management Protocol* (SNMP) (PROLEXIC, 2013).
2013	30.000 servidores DNS fizeram parte em um ataque contra a Spamhaus que atingiu picos de 300 Gbps (PRINCE, 2013). Outros ataques realizados que obtiveram um fator de amplificação próximo a 100 Gbps (RYBA et al., 2015; BREWSTER, 2013)
2014	Com um crescimento no número dos ataques DRDoS , o NTP foi explorado para realizar ataques que atingiram picos de 400 Gbps (LOPES, 2015).
2016	Mais de 150.000 dispositivos *Internet of Things* (IoT) são explorados para realizar ataques que alcançaram º 1 Tbps de tráfego (em sua grande maioria o tráfego foi gerado por *Closed-Circuit Television Camera* (CCTV)) (KHANDELWAL, 2016).
2018	Atacantes exploram servidores que deixaram serviços Memcached abertos na Internet para realizar ataques ao Github. O ataque deixou os serviços do Github indisponíveis por dois períodos de tempo e alcançou picos de º 1.4 Tbps de tráfego, sendo classificado como o maior ataque de amplificação já registrado (NEWMAN, 2018). Uma semana depois deste ataque a Netscout (BIENKOWSKI, 2018) registrou um ataque de º 1.7 Tbps de tráfego, que foi realizado pelo mesmo vetor explorado anteriormente.
2021	Nas primeiras semanas de janeiro de 2021, os ataques DRDoS contra organizações tornaram-se cada vez mais contínuos (HAQUE et al., 2022)

Fonte: Adaptado de (HEINRICH, 2019)

2.3 HONEYPOTS

Honeypots são sistemas de isca utilizados na rede para atrair invasores e atacantes para que eles utilizem esse sistema e as atividades realizadas por esses atacantes sejam capturadas para uma análise futura (BHAGAT; ARORA, 2018). No caso de ataques DRDoS honeypots são utilizados como refletores pelos atacantes para amplificar os ataques de negação de serviço.

Para um atacante, um refletor é qualquer nó na rede que envia dados para um IP em resposta a uma requisição recebida anteriormente. Refletores podem amplificar a quantidade de dados enviados, ou seja, sua resposta produz mais bytes ou pacotes, ou ambos, do que a requisição recebida. Assim, refletores potencializam o tráfego gerado por um atacante (GONDIM; ALBUQUERQUE; OROZCO, 2020).

Qualquer *host* na rede pode ser abusado como refletor, como por exemplo: servidor, *workstation* ou *honeypot*. *Honeypots*, por sua natureza, não são criados para serem acessados por usuário legítimos e sim com o objetivo de serem sondados, atacados ou até mesmo comprometidos (HOEPERS; JESSEN; CHAVES, 2007). Dessa forma, *honeypots* são extensivamente monitorados para possibilitar o estudo do comportamento e das atividades dos atacantes, levando à descoberta de novos ataques e de como ataques já conhecidos na teoria são realizados na prática (HEINRICH, 2019).

Geralmente um *honeypot* é um *host* que possui um endereço público na Internet, o qual não é anunciado. Por consequência o *host* precisa ser descoberto para a realização de qualquer tipo de interação com o sistema, o que exige algum tipo de mapeamento realizado pelos atacantes. Desta forma, é possível afirmar que qualquer interação realizada com o *honeypot* é considerada suspeita (HEINRICH, 2019).

Quanto mais funcionalidades um *honeypot* implementa e quanto mais possibilidades de interação ele oferece, maior e mais detalhado é o comportamento dos atacantes que esse *honeypot* pode observar e coletar. Um *honeypot* de baixa interatividade basicamente emula algumas funcionalidades de um sistema vulnerável, permitindo uma observação mais restrita do comportamento dos atacantes mas oferecendo um risco menor. Um *honeypot* de alta interatividade, por outro lado, permite que atacantes interajam com aplicações e serviços reais, o que oferece uma visão mais detalhada de suas atividades mas introduz um nível maior de risco (HEINRICH, 2019).

Honeypots de alta interatividade possuem mais interações e então recebem uma maior quantidade de requisições e consequentemente recolhem uma maior quantidade de *payload* que os de baixa interatividade. Um *honeypot* de alta interatividade é o HReflector Heinrich (2019) um *honeypot* quer suporta múltiplos protocolos baseados em UDP. Outro exemplo de *honeypot* de alta interatividade é o AmpPot Krämer et al. (2015) que teve a sua arquitetura utilizada como base para o desenvolvimento do HReflector.

O objetivo de expor o *honeypot* como um endereço público aberto é receber os ataques, e armazenar informações sobre eles, como quantidade de dados enviados e retornados, qual o endereço de IP (*Internet Protocol*) que enviou a requisição, entre várias outras informações que possam ser recolhidas através da requisição suspeita recebida, para após o recolher dessas informações ser possível analisar e tirar conclusões sobre o conjunto de dados. Se a rede de um *honeypot* é monitorado e o *honeypot* é abusado como refletor, é possível ver a tentativa do atacante de marcar o endereço de IP de origem como um possível invasor. Esse é um processo legítimo e natural de detecção de comportamento malicioso (HUSÁK; VIZVÁRY, 2013).

No caso de ataques DRDoS, o *honeypot* deve possuir a funcionalidade de refletor para capturar a interação dos *bots* com os refletores. Vários *honeypots* podem ser utilizados para recolher dados e assim obter a possibilidade para comparação entre os *payloads* observados pelos *honeypots* e verificar as diferenças e similaridades entre os *payloads*.

2.3.1 MP-H

2.4 TRABALHOS RELACIONADOS

Payloads de ataques DDoS e DRDoS são capturados e analisados de diversas maneiras na literatura, incluindo:

- Evolução temporal de ataques (RYBA et al., 2015; DEKA; BHATTACHARYYA; KALITA, 2017) com o auxílio da análise de *payloads*;
- Captura de *payloads* utilizando honeypots (HEINRICH; OBELHEIRO; MAZIERO, 2021; KRÄMER et al., 2015; ZHAUNIAROVICH; DODIA, 2019);
- Análise de *payload* para detecção de ataques DRDoS (XU et al., 2019; HEINRICH, 2019; DAHIYA et al., 2020)

O foco deste trabalho é a análise de *payloads* de ataques de negação de serviço capturados pelos *honeypots*. A seguir são discutidos trabalhos que possuem enfoque na coleta de dados de ataques de negação de serviço.

Rossow (2014) explorou como 14 protocolos diferentes podem ser usados em ataques de amplificação e estimou o fator de amplificação fornecido por cada um. Esse trabalho também realizou análise de tráfego: dados de fluxo de um ISP (*Internet Service Provider*) europeu foram usados para identificar vítimas e amplificadores dentro da rede, varreduras UDP para endereços *darknet* foram usadas para identificar possíveis invasores e *honeypots* foram usados principalmente para confirmar a ocorrência de ataques, sem uma análise mais profunda.

Krämer et al. (2015) realizou a introdução aos AmpPots, que são *honeypots* projetados para observar e coletar tráfego DRDoS usando nove protocolos (NTP, DNS, Chargen, SSDP, MS-SQL, NetBIOS, QOTD, SIP e SNMP). Eles analisaram dados coletados de 21 AmpPots entre fevereiro e maio de 2015, totalizando mais de 1,5 milhão de ataques, e descreveram características como duração do ataque, geolocalização da vítima e entropia de solicitação com a análise de *payloads*. Também realizaram um análise de *botnets* DDoS.

Noroozian et al. (2016) analisaram o tráfego DRDoS coletado de oito AmpPots durante 2014–2015, com um total de seis protocolos de rede (NTP, DNS, Chargen, SSDP, QOTD e SNMP). O principal objetivo do estudo é uma caracterização das vítimas de DRDoS através da análise de *payloads*, incluindo seu tipo de rede (acesso, hospedagem, empresa) e geolocalização. Eles também discutem a duração dos ataques por tipo de vítima.

Thomas, Clayton e Beresford (2017) executou uma análise de *payload* do tráfego DRDoS coletado de um grande conjunto de *honeypots* UDP para oito protocolos (QOTD, Chargen, DNS, NTP, SSDP, MS-SQL, Portmap e mDNS). A pesquisa observou mais de 5,8 milhões de ataques em um período de 1010 dias e analisaram o comportamento de varredura e várias características de ataque (duração, contagem de pacotes, número de ataques). NTP e DNS foram os protocolos mais populares, mas também notaram quantidades significativas de tráfego SSDP.

Jonker et al. (2017) efetuou a análise de tráfego DDoS usando AmpPots e tráfego de retrodifusão de um telescópio da Internet (É um sistema que permite observar tráfego na *darknet*). O trabalho observou mais de 20 milhões de ataques em dois anos (2015–2017), afetando mais de 2,2 milhões de redes. Eles também descrevem ataques conjuntos, que são ataques que empregam DRDoS e DDoS regular com endereços de origem falsificados (principalmente inundações de TCP SYN).

Heinrich, Obelheiro e Maziero (2021) elaborou uma análise de *payloads* para caracterizar ataques de múltiplos protocolos e *carpet bombing*. Além disso, o trabalho desenvolveu um *honeypot* que implementa 9 diferentes protocolos (Chargen, DNS, NTP, Memcached, QOTD, SSDP, CoAP, CLDAP, e Steam) frequentemente utilizados em ataques DRDoS. Em um período de 731 dias, o *honeypot* desenvolvido recebeu 1,8 terabyte de tráfego, contendo cerca de 20,7 bilhões de requisições que envolveram em mais de 1,4 milhões de ataques DRDoS.

Enquanto esses estudos analisam os *payloads* para investigar, caracterizar e predizer ataques distribuídos de negação de serviço, eles praticamente ignoram a evolução do conteúdo desses *payloads* de ataques ao longo do tempo. Na verdade, Rossow (2014) observa e analisa o tamanho dos *payloads* em quantidades de bytes para definir o fator de amplificação de largura de banca e também para defender e filtrar ataque de pacotes que contenham o *payload* idêntico ou próximo, contudo não chegam a analisar como o

conteúdo ou tamanho do *payload* desses ataques muda com o tempo. O diferencial desse trabalho, portanto, reside na investigação de análise temporal de evolução de *payloads* utilizados em ataques DRDoS.

2.5 CONSIDERAÇÕES DO CAPÍTULO

Ataques de negação de serviço estão cada vez mais frequentes e fáceis de se realizarem, isso apresenta um aumento de ataques DDoS ao longo dos anos. Esses ataques evoluem conforme os mecanismos de segurança também evoluem. A variedade de protocolos que podem ser usados em ataques e diferentes modos de realizar ataques como através de refletores dificultam a identificação do atacante e do ataque em questão. Embora existam diversos trabalhos que utilizam *payloads* dos ataques para a caracterização e identificação de tráfego, as características e evoluções dos *payloads* das requisições ao longo do tempo, não são discutidas na literatura.

Este trabalho propõe investigar *payloads* de ataques DRDoS de que são coletados por *honeypots*, uma ferramenta útil para compreender o funcionamento de ataques e acompanhar a evolução das técnicas usadas pelos atacantes que armazena as requisições recebidas, esses *honeypots* recebem as requisições dos atacantes através dos refletores coletam as informações em arquivos PCAP. Os *payloads* a serem analisados são os arquivos PCAP extraídos dos *honeypots*: HReflector e AmpPot.

- O *honeypot* HReflector (HEINRICH, 2019) coletou dados por aproximadamente 255 dias e suporta 7 protocolos (Chargen, DNS,Memcached, NTP, QOTD, SSDP e Steam);
- O *honeypot* AmpPot (KRÄMER et al., 2015) coletou dados por aproximadamente 485 dias e suporta 9 protocolos (QOTD, CharGen, DNS, NTP, NetBIOS, SNMP, SSDP, MSSQL, SIP)

3 PROPOSTA

Este capítulo apresenta

3.1

Nosso problema é...

Infraestrutura do honeypot

dado nossa longa data com os honeypots vamos analisar o seguinte

- análise limitada de payloads usados em ataques DRDoS - falta de análise da evolução dos payloads de ataque ao longo do tempo

4 ANÁLISE DE DADOS

Este capítulo apresenta os dados e as análises realizadas sobre especificamente 3 protocolos: NTP, DNS Memcached. Assim como análises gerais sobre todos os ataques encontrados durante o período de coleta 24/09/2018 e 11/05/2022.

4.1 IMPLANTAÇÃO

A implantação do MP-H ocorreu na rede da UDESC, em que a sua coleta aconteceu 24 horas por dia, 7 dias por semana. O *honeypot* possui um IP fixo globalmente roteável e está exporto diretamente à Internet (isto é, não está atrás de um *firewall* ou `NAT` *Network address translation*). As configurações de sistema operacional, hardware e software da máquina são as seguintes:

- Sistema operacional: Slackware Linux (kernel 4.4.14);
- Processador: AMD Phenom II X4 B93 (quatro núcleos);
- Memória RAM: 4 GB;
- Rede: Ethernet 100 Mbps;
- Servidor DNS local: Unbound (LABS, 2019);
- Servidor Memcached local: memcached.org (MEMCACHED, 2022);
- SQLite versão 3.13 (CONSORTIUM, 2016);

4.2 DEFINIÇÕES ADOTADAS

Conforme a definição de ataque adotada por (HEINRICH; LONGO; OBELHEIRO, 2017), um ataque de negação de serviço é formado por um conjunto com no mínimo 5 consultas com o mesmo IP de origem e com intervalo máximo de 60 segundos entre consultas consecutivas, e pelas respostas a essas consultas.

Uma requisição é uma consulta realizada por um atacante em um *honeypot*, para realizar um ataque. Somente requisições que são utilizadas em ataques são computadas para a análise dos dados. Requisições para varredura de portas abertas ou de fato consultas legítimas de usuários não são armazenadas no banco de dados.

Um ataque é definido como no mínimo 5 requisições para um mesmo IP de origem, o atacante modifica a sua requisição para que o IP de origem seja a vítima. Para mensurar a quantidade de novas vítimas distintas, uma métrica de "novas vítimas"é adotada em que só é computado quando um novo endereço de IP que nunca foi computado previamente

é utilizado em um ataque. Esse número tem a tendência de diminuir conforme o MP-H permanece online, pois um IP já utilizado em um ataque, caso seja utilizado novamente em um novo ataque, não é computado novamente.

O agrupamento para apresentação de dados adotados para a maioria dos gráficos foi o agrupamento de trimestres. Cada ano possui 4 trimestres e sua representação está definida como ano/trimestre, por exemplo: 2020/3 é o terceiro trimestre de 2020.

4.3 OBSERVAÇÕES GERAIS

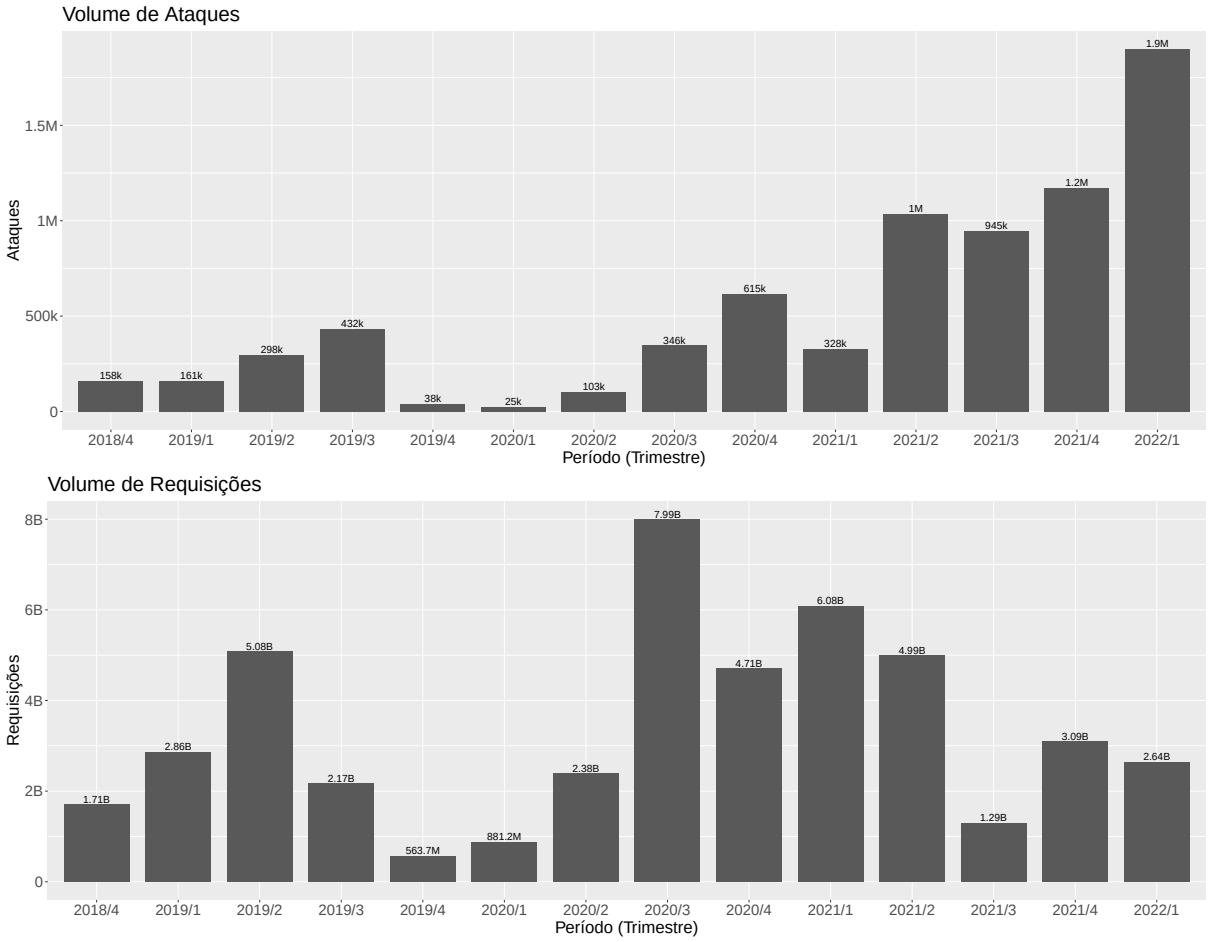
O *honeypot* MP-H durante o seu período de coleta de dados, foi possível coletar e analisar que somando todos os dados coletados, alcançamos a um total de 7.554.491 (7.54 Milhões) ataques realizados em 46.440.034.647 (46.4 Bilhões) de requisições atingindo 1.408.197 (1.4 Milhão) de vítimas (IP) distintas em um período de 1278 dias, conforme destacado por anos na Tabela 2. Conclui-se que a quantidade de novas vítimas devem decrescer de acordo com o tempo em que o MP-H permanece online, pois as vítimas que aparecem em períodos anteriores não são computadas em novos períodos.

Tabela 2 – Dados coletados. Os anos indicados com * são incompletos.

Ano	Requisições	Ataques	Novas Vítimas
2018*	1,70 B	158 k	50 k
2019	10,67 B	930 k	483 k
2020	15,96 B	1,08 M	497 k
2021	15,46 B	3,47 M	402 k
2022*	2,63 B	1,89 M	64 k

Uma grande quantidade de requisições não significa uma grande quantidade de ataques, pois um ataque contém 5 ou mais requisições (segundo definição de ataque adotada). Dessa forma, ataques e requisições não possuem uma correlação forte. Entretanto, sem requisições realizadas por atacantes, ataques não existem. A Figura 3 apresenta de forma gráfica a quantidade de ataques e requisições em cada trimestre, o gráfico na parte superior apresenta o volume de ataques e o inferior apresenta o volume de requisições. Assim, conclui-se que no período de 2020/3 foi onde houve o maior número de requisições 7,99 bilhões para 346 mil ataques o que representa que houveram ataques intensos durante esse período, e no período em que houveram mais ataques 2022/1 com 1,9 milhões de ataques houveram 2,64 bilhões de requisições representando uma maior quantidade de ataques com poucas requisições, ou seja ataques com baixa intensidade.

Figura 3 – Relação entre ataques e requisições



Fonte: Autor

4.4 AVALIAÇÃO POR PROTOCOLO

Cada protocolo tem uma forma única de ser utilizado como amplificador em ataques DRDoS. Assim, nessa seção as peculiaridades e semelhanças entre ataques que utilizam o mesmo protocolo podem ser evidenciadas.

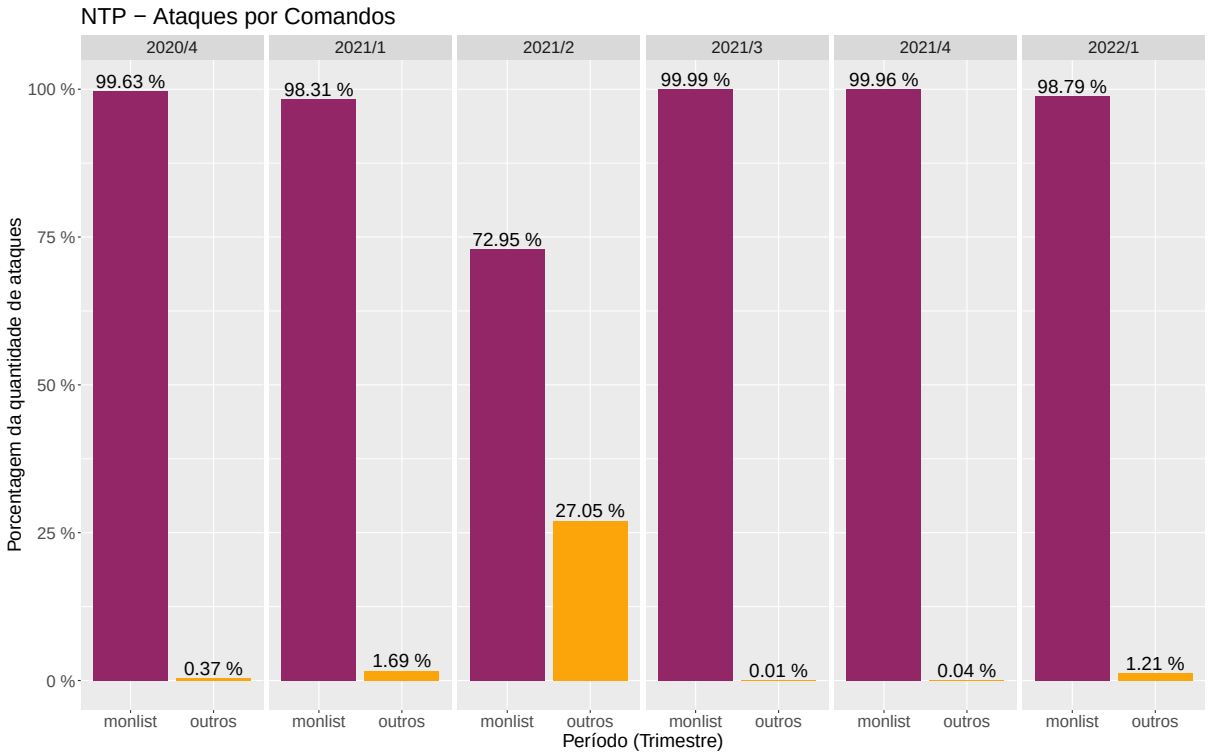
4.4.1 NTP - *Network Time Protocol*

O objetivo principal do protocolo NTP é sincronizar o horário do sistema com o servidor. O atacante utiliza como endereço de IP de origem das requisições o IP da vítima, para que a resposta da requisição seja enviada para a vítima de modo amplificado. O comando `MONLIST` nos servidores NTP vem sendo utilizado para lançar ataques, porque o `MONLIST` é uma requisição de 64 bytes considerada pequena que pode ser amplificado consideravelmente em que o comando `MONLIST` ou `MON GET LIST` reponde com uma lista de 600 sistemas que está conectado, demonstrando que o NTP é excelente para uso em ataques de amplificação (CHEEMA et al., 2022).

Estudos anteriores mostraram um predomínio de requisições `MONLIST` em ataques

DRDoS usando NTP: (HEINRICH, 2019) reportou que 99,9999% das requisições utilizadas em ataques NTP utilizaram o comando `MONLIST` em um período de 255 dias. A Figura 4 mostra a incidência de ataques com `MONLIST` em cada trimestre. Observa-se que houve mais de 99% de ataques usando `MONLIST` em todos os trimestres, com exceção de 2021/2, onde houve 27.05 % de outros ataques. Parte desse tráfego consiste em *payloads* de CLDAP e DNS enviados para a porta de destino 123/UDP; possíveis explicações são erro na configuração da ferramenta de ataque (mandando um ataque de um protocolo para a porta errada), ou tentativas de encontrar serviços em portas diferentes das portas padrão. O volume maior é de *payloads* que não obedecem ao formato de mensagens NTP, não correspondem a *payloads* de outros protocolos e para os quais não se encontrou uma explicação mesmo com análise manual. Conclui-se que os ataques NTP observados entre os períodos de 2020/4 a 2022/1 seguem a tendência histórica de uso predominante de requisições `MONLIST`.

Figura 4 – Incidência de `MONLIST` em ataques usando NTP



Fonte: Autor

4.4.2 DNS - *Domain Name System*

Servidores DNS são utilizados para traduzir nomes de domínio legíveis por humanos, como `www.example.com`, em endereços IP, como 192.0.2.44. Entretanto, uma das maneiras que atacantes utilizam esse protocolo é abusando do QTYPE `ANY`, que comumente era utilizado para depurar os servidores DNS, pois retorna com detalhes sobre subdomínios,

servidores de backup, servidores de e-mails, *aliases* e demais detalhes referentes ao domínio. O DNS é interessante a ataque de amplificação, devido a quantidade de bytes da resposta superar o tamanho da requisição. Como o DNS usa por padrão o UDP as respostas do servidor são respostas legítimas, a qual dificulta a identificação entre os pacotes legítimos enviados por usuários autorizados ou por um atacante (CHEEMA et al., 2022).

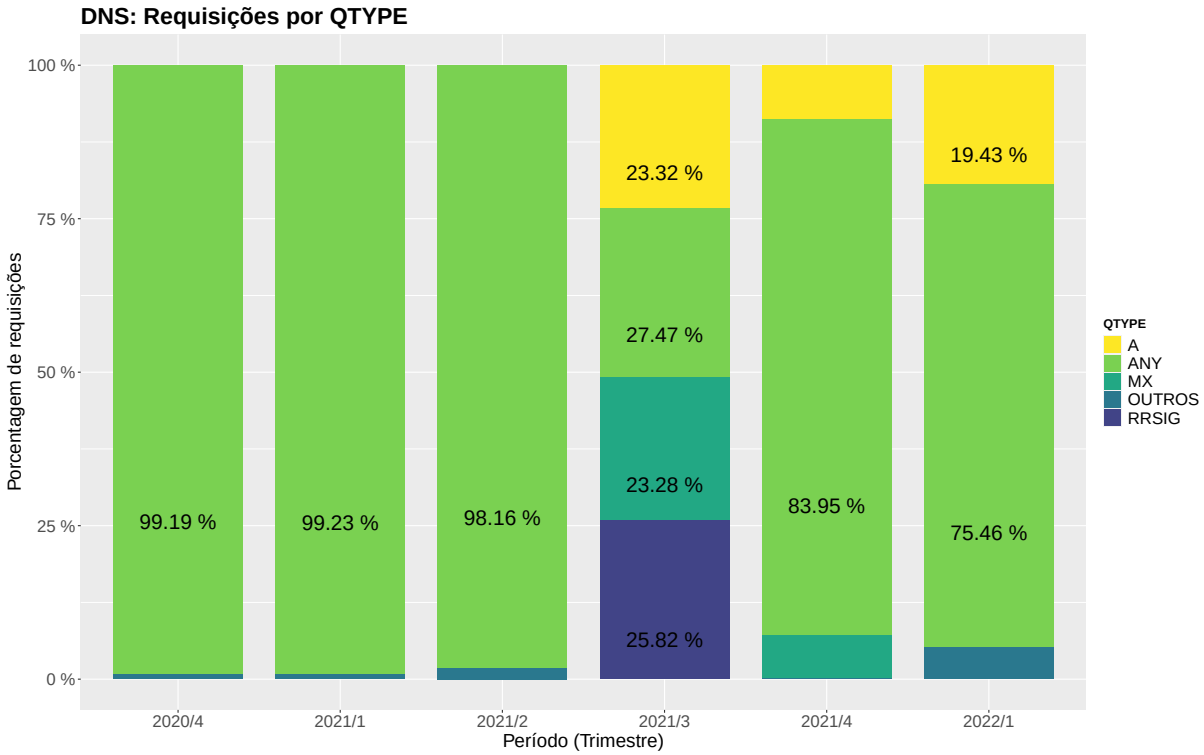
Servidores DNS armazenam informações sobre os domínios em registros de recursos (*resource records*, RRs) (HOFFMAN; SULLIVAN; FUJIWARA, 2019). Um servidor DNS possui implementações de QTYPE diferentes como `MX`, `ANY` e outros. O QTYPE `MX` (*Mail eXchanger*) foi inicialmente definido na RFC974 (PARTRIDGE, 1986) para roteamento de e-mails. Um domínio pode ter múltiplos RRs `MX`, sendo que cada `MX` tem uma prioridade definida na entrega de e-mails para o domínio (REED; REED, 2020). Consultas com QTYPE `ANY` são usadas para obter todos os RRs com mesmo QNAME, independente de seu QTYPE (HEINRICH, 2019). Quando um QNAME possui um conjunto grande de RRs, o uso de `ANY` retorna uma resposta muito maior do que a consulta, o que é explorado em ataques DRDoS para obter amplificação.

Estudos anteriores mostraram um predomínio de requisições DNS com QTYPE `ANY` em ataques DRDoS. Como (HEINRICH, 2017) apresenta uma predominância de 93,7% do QTYPE `ANY` nas consultas realizadas entre 17/09/2016 e 25/05/2017. Além disso com dados de 2018 e 2019 (HEINRICH, 2019) apresentou uma dominância ainda maior, 99,8% das consultas utilizadas em ataques eram do QTYPE `ANY`, por fim, somente com dados de 2019 (ANAGNOSTOPOULOS; LAGOS; KAMBOURAKIS, 2022) observou que cerca de 99% de todo o tráfego de ataques é exclusivo de `ANY`. Inclusive, esse predomínio levou, em 2019, à adoção da RFC 8482 (ABLEY et al., 2019), que define diretrizes para que servidores DNS limitem o tamanho de respostas a requisições `ANY`, reduzindo assim a amplificação proporcionada por esse tipo de requisição.

Para analisar se o predomínio de `ANY` se mantém, ou se houve adaptação por parte dos atacantes, a Figura 5 mostra, para cada trimestre, a porcentagem de QTYPEs usados em requisições DNS associadas a ataques. Observa-se que houve uma predominância nas requisições dos ataques usando `ANY` em todos os trimestres, com exceção de 2021/3. Entre 2020/4 e 2021/2, mais de 98% das requisições tinham QTYPE `ANY`. O uso de `ANY` passou a cair desde 2021/4, chegando a pouco mais de 75% em 2022/1. Há uma discrepância em 2021/3, que pode ser atribuída em parte a uma redução de 91,9% no volume de requisições DNS, de 15,8 M em 2021/2 para 1,2 M em 2021/3. As evidências indicam então que os ataques DRDoS usando DNS vêm migrando do QTYPE `ANY` para os QTYPEs `A` e `MX`. Essa adaptação, no entanto, é gradativa: ela torna-se evidente quase três anos após a publicação da RFC 8482, e a maioria das requisições de ataque ainda usam `ANY`.

Outra questão que pode ser examinada é por quanto tempo os mesmos RRs são usados em ataques DRDoS. Mudanças no espaço de nomes do DNS são naturais: novos

Figura 5 – Requisições DNS por `QTYPE`



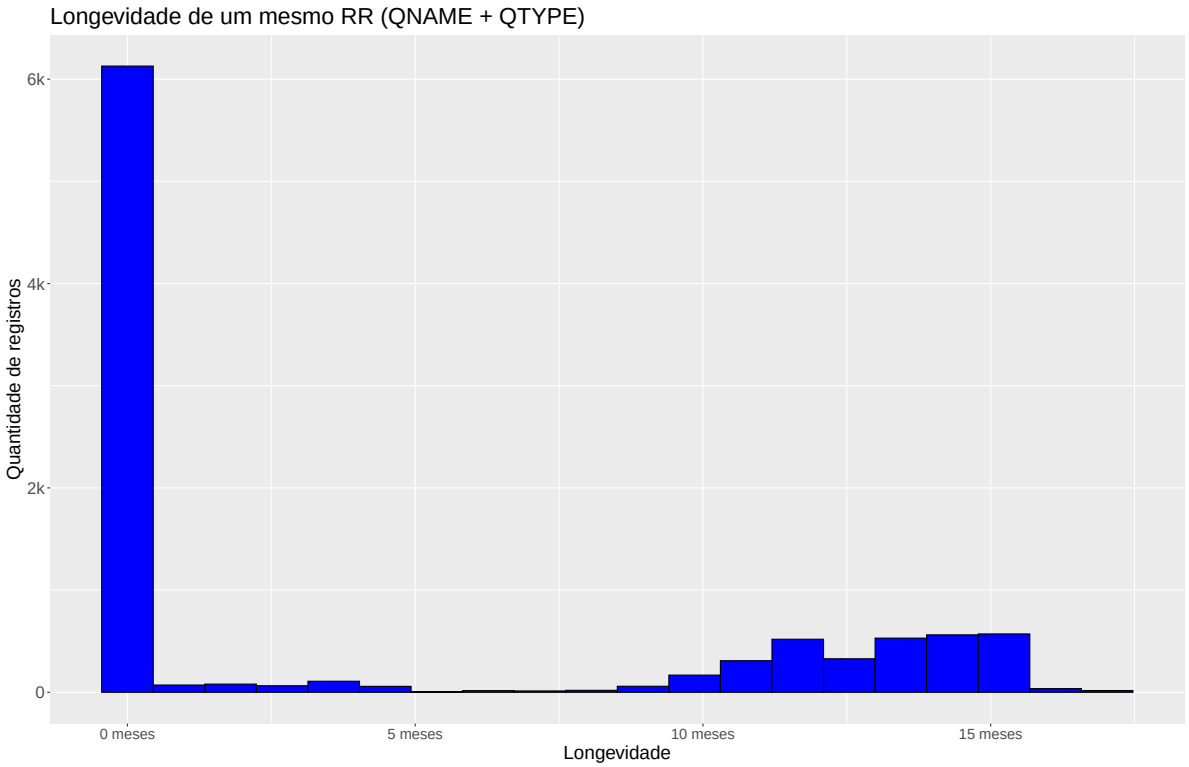
Fonte: Autor

nomes e domínios são criados, nomes e domínios existentes podem ser removidos, domínios podem passar por alterações (como a adoção de DNSSEC). Nomes usados frequentemente em ataques podem levar à reconfiguração de seus respectivos domínios visando a reduzir do tamanho das respostas. No conjunto de dados sob análise, a longevidade de um RR pode ser definida como o intervalo entre a primeira e a última aparição desse RR em ataques. A Figura 6 mostra um histograma da longevidade dos RRs observados. Dos 9.663 RRs distintos, 6.048 (62,59%) têm longevidade curta (um dia ou menos), 670 (6,93%) RRs têm longevidade entre um dia e 10 meses, e 2.945 (30,48%) possuem alta longevidade, superior a 10 meses. Entre os RRs com alta longevidade, 79,5% utilizam o QTYPE `A`.

Na literatura não é encontrado abordagens apresentação de dados referentes a longevidade de RR *Resource Records* em ataques DNS. As observações encontradas focam em apresentar quanto tempo um mesmo domínio recebe ataques continuamente, por exemplo o `QNAME` "peacecorps.gov."do QTYPE `ANY` teve o primeiro ataque registrado em 31/10/2020 e o ultimo ataque com o mesmo "QNAME"e "QTYPE"em 11/02/2022 completando uma longevidade de aproximadamente um ano e três meses (40 milhões de segundos) com um total de 106.781 ataques diferentes somando 72,3 milhões de requisições utilizando o mesmo RR nesse período.

Observou-se que alguns domínios continuam a ser utilizados em ataques de amplificação e assim aumentando a sua longevidade, conforme apresentado na Tabela 3

Figura 6 – Longevidade de RRs em ataques DNS



Fonte: Autor

em que é realizado uma comparação dos domínios mais utilizados em ataques DRDoS, mesmo com posições distantes no ranking de utilização comparados aos outros trabalhos, ainda representa que os domínios continuam a ser utilizados. Conclui-se que os RRs com longevidade inferior a um dia foram usados em um conjunto reduzido de ataques (99% deles foram utilizados em somente um ataque). Por fim, dos 2.945 RRs que possuem alta longevidade (maior que 10 meses) 2.300 (78,09%) são do QTYPE `A`, 637 (21,62%) do QTYPE `MX` e somente 5 (0,16%) do QTYPE `ANY`.

Tabela 3 – RRs ordenados pela quantidade de consultas

RR		Referência		Posição Referência	Posição Atual
`1x1.cz`	`ANY`	(HEINRICH, 2019)	`ANY`	2	3619
`1x1.cz`	`ANY`	(HEINRICH, 2017)	`ANY`	5	3619
`.`	`ANY`	(HEINRICH, 2017)	`ANY`	6	1918
`.`	`RRSIG`	(HEINRICH, 2017)	`ANY`	6	3167
`.`	`A`	(HEINRICH, 2017)	`ANY`	6	3429
`commerce.gov`	`ANY`	(HEINRICH, 2017)	`A`	8	10517
`cpsc.gov`	`ANY`	(HEINRICH, 2017)	`A`	100	3335

Além dos domínios já reportados por outros trabalhos, os RRs apresentados na Tabela 4 são os registros com maior longevidade captados pelo MP-H. Os registros foram analisados e 9 domínios do top 10 são do subdomínio `".ae"` e do QTYPE `MX`, porém

Tabela 4 – Top 10 RRs com maior longevidade

RR		Ataques	Longevidade
`ambulance.gov.ae`	`MX`	69	510,7 dias
`ncc.ae`	`MX`	39	509,2 dias
`szgmc.gov.ae.`	`MX`	22	508,9 dias
`dc.gov.ae.`	`MX`	27	507,3 dias
`fca.gov.ae.`	`MX`	58	506,4 dias
`dans.gov.ae.`	`MX`	37	505,8 dias
`almajles.gov.ae.`	`MX`	39	505,5 dias
`investbank.ae.`	`MX`	40	504,7 dias
`tstng.net.`	`A`	39	504,4 dias
`pwad.gov.ae.`	`MX`	58	504,2 dias

nenhum deles possui uma amplificação significativa, apesar da longa longevidade dos RRs não necessariamente significa que possuem uma grande quantidade de ataques. O primeiro RR com maior longevidade do QTYPE `ANY` é o `"sl."` com 24.782 ataques e uma longevidade de 490,7 dias, esse domínio possui uma amplificação significativa.

Toda consulta DNS possui um `TxID` aleatório que é utilizado pelo cliente para verificar uma resposta com a requisição correspondente, e para identificar retransmissões. Como o `TxID` tem 16 bits, ele pode assumir qualquer valor entre 0 e 65535. Se os `IDs` forem equiprováveis, a probabilidade de que o `TxID` assuma um determinado valor é 1/65536. Assim, em um conjunto de N requisições, o valor esperado para o número de repetições de um `TxID` é de N/65536. Um número de repetições muito acima do valor esperado indica que um cliente não usa um `TxID` aleatório para cada requisição, mas `IDs` fixos, ou que são alterados apenas de tempos em tempos.

Foi observado que vários ataques utilizavam o mesmo `TxID`, como apresentado na Tabela 5 em que o top 5 `TxID` que mais repetiram em requisições de um mesmo domínio, então para o "17767"de domínio "isc.org."em 2.63 milhões de requisições utilizadas em ataques, era probabilisticamente uma repetição de `TxID` de 40 vezes, contudo entre todas as requisições o `TxID` repetiu 52.559 vezes.

Tabela 5 – Repetições de TxID em ataques DNS

`TxID`	**`QNAME`**	**Requisições**	**Repetição Observada**	**Repetição Esperada**
17767	isc.org.	2.63 M	52.559	40
26566	peacecorps.gov.	9 M	34.570	137
17767	sl.	5.9 M	24.740	90
1	pizzaseo.com.	325 k	4.154	4
16049	irs.gov.	17 k	1.051	0,26

Fonte: Autor

Além da repetição do `TxID` em um mesmo domínio, é incomum observar múltiplos

domínios utilizando o mesmo `TxID`. Como o `TxID` de número "17767"que foi utilizado em 87.924 ataques de DNS totalizando 9.038.301 requisições com o mesmo `TxID` entre cerca de 8 domínios diferentes.

Conclui-se, que além do grande número de ataques utilizando o mesmo `TxID` e também a sobreposição entre os ataques sendo executados em um mesmo período sugerem que muitos deles utilizaram a mesma ferramenta para realizar os ataques. Pois os atacantes não realizaram o trabalho de alterar o `TxID` ou utilizar um número randômico ou incremental para que o `TxID` fosse diferente entre seus ataques.

4.4.3 Memcached

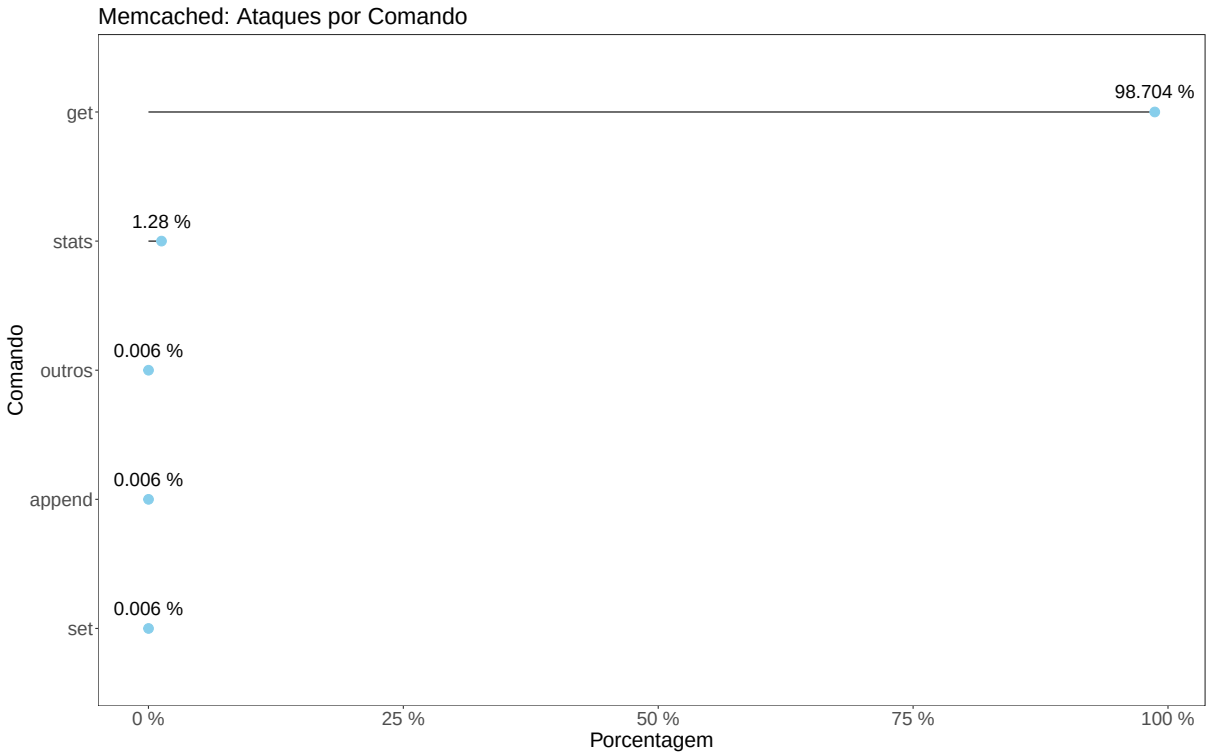
Memcached é um armazenamento de chave-valor em memória para dados pequenos como *Strings* e objetos provenientes de chamadas de banco de dados ou de APIs ou até renderização de páginas (MEMCACHED, 2022). Todos os comandos são implementados para ser o mais rápido possível, isso permite uma alta velocidade nas execuções para todos os casos. Os principais comandos do protocolo utilizado em ataques DRDoS são:

- `set` O comando mais comum, salva o dado e sobrescreve qualquer dado que já esteja salvo com essa chave.
- `get` O comando utilizado para buscar os dados salvos pelo comando "`set`".
- `stats` O comando utilizado para consultar dados do servidor memcached.

O protocolo Memcached produz a maior amplificação possível de todos os protocolos vulneráveis conhecidos (BURKE; HERBERT; MOOI, 2018). De acordo com (CISA, 2019) o protocolo tem um fator de amplificação de até 51.000 vezes, isso significa que para cada byte de dado enviado pelo atacante, o serviço de Memcached pode responder com um volume de até 51 kilobytes de dados. Um grande fator de amplificação reduz a quantidade de bots necessário pelo atacante para lançar um ataques DDoS com sucesso.

Observou-se que o comando "`get`"era predominante em um trabalho anterior (HEINRICH, 2019) em que cerca de 91,6% dos *payloads* distintos do protocolo Memcached utilizados em ataques, eram realizados com o comando "`get`"ou "`set`". Assim, analisando dados de 29/10/2020 até 11/05/2022 foi possível reafirmar a predominância do comando "`get`"na utilização de ataques do protocolo Memcached, a Figura 7 apresenta que 17.719 (98,8%) dos ataques utilizaram "`get`"para realizar a amplificação em seus ataques, e somente 209 (1,16%) o comando "`stats`", os outros comandos foram utilizados em 1 ou 2 ataques. Por fim, conclui-se que o comando "`get`"é o comando mais utilizado em ataques DRDoS.

Figura 7 – Relação de ataques e comandos



Fonte: Autor

4.4.4 CoAP

O `CoAP` (*Constrained Application Protocol*) é um protocolo UDP de transferência para uso de servidores pequenos com com pouca força e baixo poder computacional como a comunicação entre dispositivos na Internet das Coisas (*Internet of Things*, `IoT`). Além disso, fornece um modelo de interação com requisição e resposta entre aplicações, assim como suporte à descoberta integrada de serviços e recursos e inclui conceitos-chave da Web, como *URIs* e tipos de mídia da Internet. O CoAP foi projetado para interagir facilmente com HTTP para integração com a Web, atendendo a requisitos especializados, como suporte *multicast* e simplicidade para ambientes restritos.(SHELBY; HARTKE; BORMANN, 2014).

Trabalhos anteriores como (UTECH; OBELHEIRO, 2020) apresenta a utilização de CoAP em DRDoS com 6 meses de coleta de dados utilizando o MP-H foram registrados apenas 28 ataques, estes ataques tiveram um total de 73.116 requisições. Ao utilizar o mesmo *honeypot* para coletar dados por mais tempo como 21 meses entre 2020/1 até 2021/4 foram registrados 4.205 ataques em 2.017.192 requisições atingindo 3.860 vítimas distintas. A URI mais utilizada em ataques utilizando CoAP é `"*.well-known"` sendo utilizada 2.813 vezes (71,78%), o outro *payload* é um *token* com número específico `"d19796c1"` que se repete 1.106 vezes (28,28%), nenhuma informação adicional sobre o *token* foi encontrada. Os *tokens* em CoAP de modo legítimo são utilizados para que seja possível identificar a

resposta de uma requisição, pois o servidor responde a uma consulta com o mesmo *token* enviado para a consulta.

4.4.5 CLDAP

O protocolo `CLDAP` *(Connection-less Lightweight Directory Access Protocol)* foi projetado para fornecer acesso a diretório sem incorrer nos requisitos de recursos do `DAP` *(Directory Access Protocol)*. Em geral, o protocolo tem o objetivo de evitar o tempo decorrido associado à comunicação orientada à conexão e facilitar o uso de diretório de maneira análoga ao `DNS`. Destina-se especificamente a aplicativos de pesquisa simples que requerem a leitura de um pequeno número de valores de atributos de uma única entrada (YOUNG, 1995).

Este protocolo tem um fator de amplificação de 56 até 70 vezes, para cada byte enviado pelo atacante a vítima recebe 70 bytes de dados (SUBRAMANI; PERDISCI; KONTE, 2021). `CLDAP` tem sido utilizado em grandes ataques de amplificação como por exemplo um dos maiores ataques já registrado de negação de serviço com pico de 2.3 Tbps de dados contra a `AWS` *(Amazon Web Services)* em 2020 (SNEHI; BHANDARI, 2021).

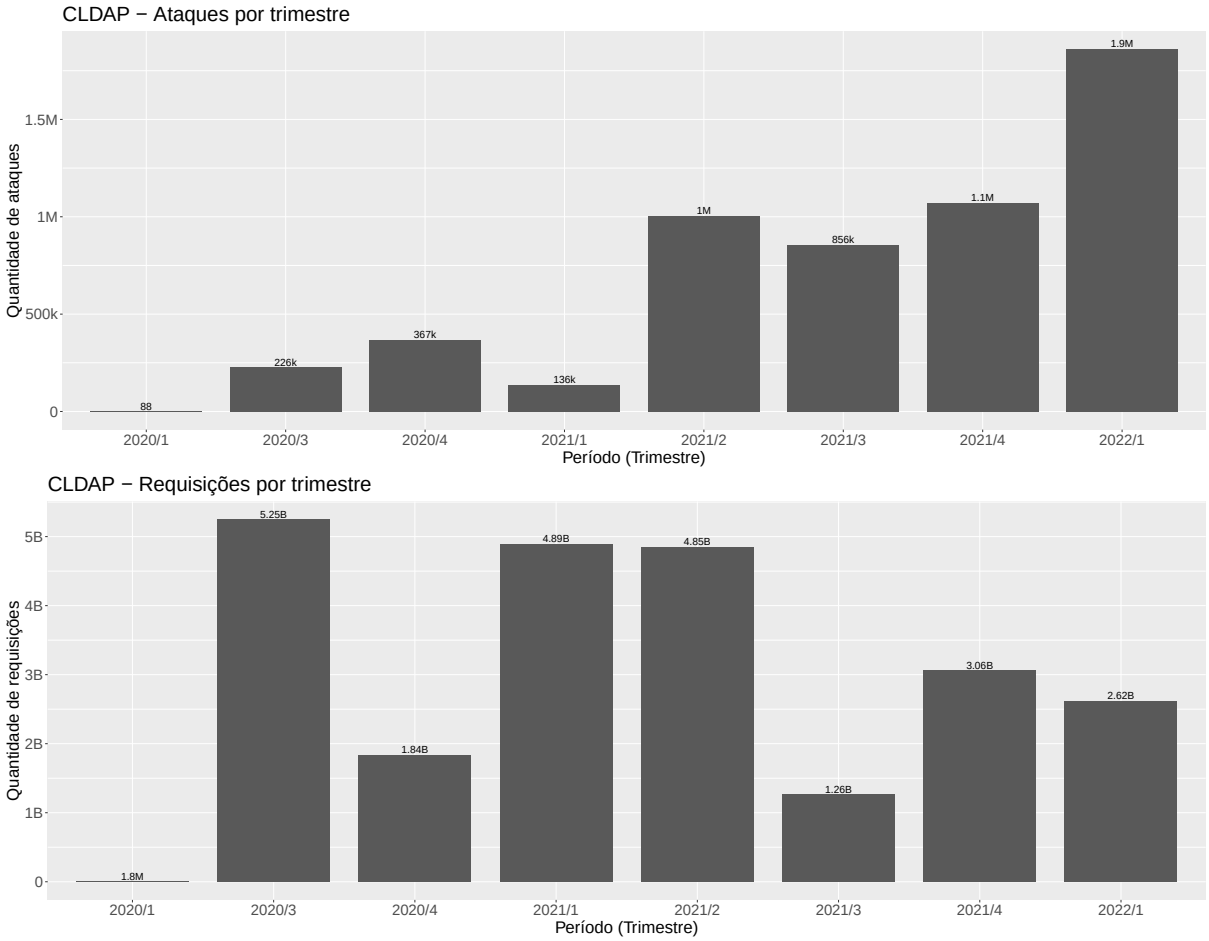
O suporte ao protocolo `CLDAP` foi adicionado ao MP-H em 10/07/2020 e dados foram coletados até 31/03/2022, nesse período ocorreram 5,5 milhões de ataques que acumulam 23,7 bilhões de requisições para 631 mil vítimas distintas. Ao observar o *payload* de dados do `CLDAP`, foi constatado que 51,69% utilizaram `"objectclass0"` que significa uma especificação de filtro vazio, basicamente os atacantes não especificaram nenhum filtro para obter todos os registros possível pelo protocolo e obter uma maior amplificação caso filtrasse por algum atributo.

Os registros do protocolo `CLDAP` agrupados por trimestres apresentados na Figura 8 mostram a dispersão dos 5,5 M de ataques e 23,7 B de requisições em 8 trimestres de 2020/1 até 2022/1. Conforme observado na figura, é possível destacar que nos três últimos trimestres (2021/3, 2021/4 e 2022/1) a relação da quantidades de requisições por ataques diminuiu cerca de 90% com uma média de 17.983 requisições por ataque durante os cinco primeiros trimestres, para 1.912 requisições por ataque nos três últimos trimestres, isso representa que os ataques realizados nesse período são ataques de baixa intensidade.

4.4.6 SSDP

O protocolo *Simple Service Discovery Protocol* `(SSDP)` fornece um mecanismo de descoberta de usuários na rede, com pouca ou nenhuma configuração estática, é possível descobrir serviços presentes na rede, isso é possível devido ao protocolo fornecer suporte a descoberta *multicast*, além do roteamento entre os dispositivos (GOLAND, 1999). Como esse protocolo exige pouca configuração do dispositivo, qualquer dispositivo em casas ou

Figura 8 – Relação de ataques e requisições CLDAP



Fonte: Autor

escritório está apto a utilizar esse protocolo, como impressoras, televisores, celulares, caixas de som.

O protocolo não verifica se o dispositivo que enviou a solicitação de pesquisa reside na mesma rede que o dispositivo raiz. Portanto, cada pacote IP com endereços *unicast* como origem ou destino pode ser roteado pela Internet (ANAGNOSTOPOULOS; LAGOS; KAMBOURAKIS, 2022). Como o `SSDP` é utilizado em milhões de pequenos escritórios e dispositivos domésticos, é um desafio atualizar as configurações e evitar ataques de amplificação por meio dessa infraestrutura (HYSLIP; HOLT, 2019).

O dispositivo explorado em ataques DRDoS com o protocolo `SSDP` que responde a requisição pode gerar um fator de amplificação de até 38 vezes (GONDIM; ALBUQUERQUE; OROZCO, 2020). Ao observar um trabalho anterior que também utilizou dados coletados do MP-H de setembro de 2018 á junho de 2019 (255 dias), foi possível observar que as consultas do `SSDP` foram focadas em amplificação de tráfego: 99,9% das requisições foram buscas por dispositivos utilizando *M-SEARCH* (HEINRICH, 2019). Ao realizar a pesquisa novamente com uma coleta de dados mais longa (1276 dias) de fevereiro de

2018 à março de 2022, a conclusão do payload utilizado em ataques DRDoS abusando do protocolo `SSDP` permanece a mesma, pois 99,8% das requisições utilizaram o *M-SEARCH*.

5 CONCLUSÃO

REFERÊNCIAS

ABLEY, J. et al. *Providing minimal-sized responses to DNS Queries That Have QTYPE= ANY*. [S.l.], 2019. Citado na página 21.

ALIEYAN, K. et al. An overview of ddos attacks based on dns. In: . [S.l.: s.n.], 2016. Citado na página 5.

ANAGNOSTOPOULOS, M.; LAGOS, S.; KAMBOURAKIS, G. Large-scale empirical evaluation of dns and ssdp amplification attacks. *Journal of Information Security and Applications*, Elsevier, v. 66, p. 103168, 2022. Citado 2 vezes nas páginas 21 e 28.

BHAGAT, N.; ARORA, B. Intrusion detection using honeypots. In: IEEE. *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*. [S.l.], 2018. p. 412–417. Citado na página 12.

BIENKOWSKI, T. *No sooner did the ink dry: 1.7 tbps DDoS attack makes history*. [S.l.]: March, 2018. Citado na página 11.

BREWSTER, T. *Cyber Attacks Strike Zimbabweans Around Controversial Election*. [S.l.]: August, 2013. Citado na página 11.

BURKE, I. D.; HERBERT, A.; MOOI, R. Using network flow data to analyse distributed reflection denial of service (drdos) attacks, as observed on the south african national research and education network (sanren) a postmortem analysis of the memcached attack on the sanren. In: *Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists*. [S.l.: s.n.], 2018. p. 164–170. Citado na página 25.

CERT, S. A. *CERT: http://www. cert. org/advisories*. [S.l.], 1998. Citado na página 11.

CERT.BR. Recomendações para melhorar o cenário de ataques distribuídos de negação de serviço (ddos). *https://www.cert.br/docs/whitepapers/ddos/*, 2016. Citado na página 4.

CHEEMA, A. et al. Prevention techniques against distributed denial of service attacks in heterogeneous networks: A systematic review. *Security and Communication Networks*, Hindawi, v. 2022, 2022. Citado 2 vezes nas páginas 19 e 21.

CHEN, X. et al. Preventing drdos attacks in 5g networks: a new source ip address validation approach. In: IEEE. *GLOBECOM 2020-2020 IEEE Global Communications Conference*. [S.l.], 2020. p. 1–6. Citado na página 10.

CISA, C. . I. S. A. *UDP-Based Amplification Attacks | CISA*. 2019. <https://www.cisa.gov/uscert/ncas/alerts/TA14-017A>. (Accessed on 10/25/2022). Citado na página 25.

CONSORTIUM, S. *SQLite Release 3.13.0 On 2016-05-18*. 2016. <https://www.sqlite.org/releaselog/3_13_0.html>. (Accessed on 10/28/2022). Citado na página 17.

CORNELL. *18 U.S. Code § 1030 - Fraud and related activity in connection with computers | U.S. Code | US Law | LII / Legal Information Institute*. 1984. Disponível em: <https://www.law.cornell.edu/uscode/text/18/1030>. Citado na página 11.

COX, J. *The History of DDoS Attacks as a Tool of Protest*. 2014. <https://www.vice.com/en/article/d734pm/history-of-the-ddos-attack>. (Accessed on 01/09/2022). Citado na página 11.

DAHIYA, A. et al. Honeynetbased defensive mechanism against ddos attacks. *International Journal of Information Security Science*, v. 9, n. 3, p. 140–153, 2020. Citado na página 13.

DEAR, B. Perhaps the first denial-of-service attack. *PLATO History Blog*, 2010. Citado na página 11.

DEKA, R. K.; BHATTACHARYYA, D. K.; KALITA, J. K. Ddos attacks: Tools, mitigation approaches, and probable impact on private cloud environment. *Big Data Analytics for Internet of Things*, Wiley Online Library, p. 285–319, 2017. Citado na página 13.

GOLAND, Y. Y. Simple service discovery protocol/1.0 operating without on arbiter. *IETF INTERNET-DRAFT draft-cai-ssdp-v1-03. txt*, 1999. Citado na página 27.

GONDIM, J. J.; ALBUQUERQUE, R. de O.; OROZCO, A. L. S. Mirror saturation in amplified reflection distributed denial of service: A case of study using snmp, ssdp, ntp and dns protocols. *Future Generation Computer Systems*, Elsevier, v. 108, p. 68–81, 2020. Citado 3 vezes nas páginas 4, 12 e 28.

HAQUE, M. R. et al. Unprecedented smart algorithm for uninterrupted sdn services during ddos attack. *Computers, Materials & Continua*, Tech Science Press, v. 70, n. 1, p. 875–894, 2022. Citado na página 11.

HEINRICH, T. Análise longitudinal de dados do dnspot. In: . [S.l.: s.n.], 2017. Citado 2 vezes nas páginas 21 e 23.

HEINRICH, T. *Caracterizaçao de Ataques DRDoS Usando Honeypot*. Tese (Doutorado) — Dissertaçao de mestrado em Computaçao Aplicada, UDESC, Joinville (SC), 2019. Citado 7 vezes nas páginas 5, 6, 12, 13, 15, 25 e 28.

HEINRICH, T. Caracterização de ataques drdos usando honeypot. In: . [s.n.], 2019. Disponível em: <https://www.udesc.br/arquivos/cct/id_cpmenu/1024/Disserta___o_completa_15699280495759_1024.pdf>. Citado 6 vezes nas páginas 10, 11, 12, 20, 21 e 23.

HEINRICH, T.; LONGO, F. de S.; OBELHEIRO, R. R. Experiências com um honeypot dns: Caracterização e evolução do tráfego malicioso. In: SBC. *Anais do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. [S.l.], 2017. p. 292–305. Citado na página 17.

HEINRICH, T.; OBELHEIRO, R. R.; MAZIERO, C. A. New kids on the drdos block: Characterizing multiprotocol and carpet bombing attacks. In: SPRINGER. *International Conference on Passive and Active Network Measurement*. [S.l.], 2021. p. 269–283. Citado 3 vezes nas páginas 6, 13 e 14.

HOEPERS, C.; JESSEN, K. S.; CHAVES, M. Honeypots e honeynets: Definições e aplicações. *Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança*

no Brasil, ver, 2007. Disponível em: <https://www.cert.br/docs/whitepapers/honeypots-honeynets/#ref-02>. Citado 2 vezes nas páginas 6 e 12.

HOFFMAN, P.; SULLIVAN, A.; FUJIWARA, K. *RFC 8499: DNS Terminology*. [S.l.], 2019. Citado na página 21.

HUSÁK, M.; VIZVÁRY, M. Poster: Reflected attacks abusing honeypots. In: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. [S.l.: s.n.], 2013. p. 1449–1452. Citado 2 vezes nas páginas 6 e 13.

HYSLIP, T. S.; HOLT, T. J. Assessing the capacity of drdos-for-hire services in cybercrime markets. *Deviant Behavior*, Taylor & Francis, v. 40, n. 12, p. 1609–1625, 2019. Citado na página 28.

JONKER, M. et al. Millions of targets under attack: a macroscopic characterization of the dos ecosystem. In: *Proceedings of the 2017 Internet Measurement Conference*. [S.l.: s.n.], 2017. p. 100–113. Citado 2 vezes nas páginas 4 e 14.

KHANDELWAL, S. World's largest 1tbps ddos attack launched from 152,000 hacked smart devices. *The Hacker News*, 2016. Citado na página 11.

KRÄMER, L. et al. Amppot: Monitoring and defending against amplification ddos attacks. In: SPRINGER. *International Symposium on Recent Advances in Intrusion Detection*. [S.l.], 2015. p. 615–636. Citado 5 vezes nas páginas 6, 12, 13, 14 e 15.

LABS, S. N. *NLnet Labs - Unbound - About*. 2019. <https://nlnetlabs.nl/projects/unbound/about/>. (Accessed on 10/28/2022). Citado na página 17.

LEMOS, R. *History Shows DDoS Volumes to Keep Rising Despite Mitigation Efforts*. 2018. <https://www.eweek.com/security/how-ddos-attacks-techniques-have-evolved-over-past-20-years/>. (Accessed on 01/09/2022). Citado na página 11.

LONG, N.; THOMAS, R. Trends in denial of service attack technology. *CERT Coordination Center*, v. 648, p. 651, 2001. Citado na página 8.

LOPES, R. W. *Ataques DDoS Panorama, Mitigação e Evolução*. 2015. <https://ftp.registro.br/pub/gter/gter39/08-AtaquesDdosPanoramaMitigacaoEvolucao.pdf>. (Accessed on 01/09/2022). Citado na página 11.

MEMCACHED. *memcached - a distributed memory object caching system*. 2022. <https://memcached.org/>. (Accessed on 10/25/2022). Citado 2 vezes nas páginas 17 e 25.

MIRKOVIC, J.; REIHER, P. A taxonomy of ddos attack and ddos defense mechanisms. *ACM SIGCOMM Computer Communication Review*, ACM New York, NY, USA, v. 34, n. 2, p. 39–53, 2004. Citado na página 9.

NEWMAN, L. H. Github survived the biggest ddos attack ever recorded. *Wired*, v. 1, 2018. Citado na página 11.

NIST. *NVD - CVE-1999-1379*. 1999. <https://nvd.nist.gov/vuln/detail/CVE-1999-1379>. (Accessed on 01/09/2022). Citado na página 11.

NOROOZIAN, A. et al. Who gets the boot? analyzing victimization by ddos-as-a-service. In: SPRINGER. *International Symposium on Research in Attacks, Intrusions, and Defenses*. [S.l.], 2016. p. 368–389. Citado na página 14.

PARTRIDGE, C. *Mail routing and the domain system*. [S.l.], 1986. Citado na página 21.

PAXSON, V. An analysis of using reflectors for distributed denial-of-service attacks. *ACM SIGCOMM Computer Communication Review*, ACM New York, NY, USA, v. 31, n. 3, p. 38–47, 2001. Citado 2 vezes nas páginas 4 e 5.

PRINCE, M. *The DDoS That Almost Broke the Internet. blog. cloudflare. com/the-ddos-that-almost-broke-the-internet*. [S.l.]: March, 2013. Citado na página 11.

PROLEXIC. *Distributed Reflection Denial of Service (DRDoS) Attacks An Introduction to the DrDoS White Paper Series*. 2013. <https://news.asis.io/sites/default/files/Distributed_Reflection_DoS_Attacks_White_Paper_A4_031513.pdf>. (Accessed on 11/09/2021). Citado na página 11.

RANGAPUR, A.; KANAKAM, T.; JUBILSON, A. DDoSDet: An approach to detect DDoS attacks using neural networks. *arXiv preprint arXiv:2201.09514*, 2022. Citado na página 4.

REED, J. A.; REED, J. Potential email compromise via dangling dns mx. 2020. Citado na página 21.

ROSSOW, C. Amplification hell: Revisiting network protocols for ddos abuse. In: *NDSS*. [S.l.: s.n.], 2014. Citado 5 vezes nas páginas 4, 6, 10, 13 e 14.

RYBA, F. J. et al. Amplification and drdos attack defense–a survey and new perspectives. *arXiv preprint arXiv:1505.07892*, 2015. Citado 2 vezes nas páginas 11 e 13.

SHELBY, Z.; HARTKE, K.; BORMANN, C. *The constrained application protocol (CoAP)*. [S.l.], 2014. Citado na página 26.

SNEHI, M.; BHANDARI, A. Vulnerability retrospection of security solutions for software-defined cyber–physical system against ddos and iot-ddos attacks. *Computer Science Review*, Elsevier, v. 40, p. 100371, 2021. Citado na página 27.

SUBRAMANI, K.; PERDISCI, R.; KONTE, M. Detecting and measuring in-the-wild drdos attacks at ixps. In: SPRINGER. *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. [S.l.], 2021. p. 42–67. Citado na página 27.

THOMAS, D. R.; CLAYTON, R.; BERESFORD, A. R. 1000 days of udp amplification ddos attacks. In: IEEE. *2017 APWG Symposium on electronic crime research (eCrime)*. [S.l.], 2017. p. 79–84. Citado 2 vezes nas páginas 4 e 14.

UTECH, G. R.; OBELHEIRO, R. R. Investigando o uso de coap em ataques drdos. In: SBC. *Anais da XVIII Escola Regional de Redes de Computadores*. [S.l.], 2020. p. 103–108. Citado na página 26.

WELZEL, A.; ROSSOW, C.; BOS, H. On measuring the impact of ddos botnets. In: *Proceedings of the Seventh European Workshop on System Security*. [S.l.: s.n.], 2014. p. 1–6. Citado na página 4.

WOODY, C.; MEAD, N.; SHOEMAKER, D. Foundations for software assurance. In: IEEE. *2012 45th Hawaii International Conference on System Sciences*. [S.l.], 2012. p. 5368–5374. Citado na página 11.

XU, R. et al. A drdos detection and defense method based on deep forest in the big data environment. *Symmetry*, Multidisciplinary Digital Publishing Institute, v. 11, n. 1, p. 78, 2019. Citado na página 13.

YOUNG, A. *Connection-less lightweight X. 500 directory access protocol*. [S.l.], 1995. Citado na página 27.

ZETTER, K. Lazy hacker and little worm set off cyberwar frenzy. *Wired News. http://www. wired. com/threatlevel/2009/07/mydoom*, 2009. Citado na página 11.

ZHAUNIAROVICH, Y.; DODIA, P. Sorting the garbage: filtering out drdos amplification traffic in isp networks. In: IEEE. *2019 IEEE Conference on Network Softwarization (NetSoft)*. [S.l.], 2019. p. 142–150. Citado na página 13.