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

RAFAEL TENFEN

CARACTERIZAÇÃO DA EVOLUÇÃO DO USO DE PROTOCOLOS EM ATAQUES DRDOS COM BASE EM DADOS DE HONEYPOTS

JOINVILLE
2023

RAFAEL TENFEN

CARACTERIZAÇÃO DA EVOLUÇÃO DO USO DE PROTOCOLOS EM ATAQUES DRDOS COM BASE EM DADOS DE HONEYPOTS

Dissertação apresentada ao Programa de Pós–Graduação em Computação Aplicada do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina, como requisito parcial para a obtenção do grau de Mestre em Computação Aplicada.

Orientador: Dr. Rafael Rodrigues Obelheiro

JOINVILLE
2023

Para gerar a ficha catalográfica de teses e
dissertações acessar o link:
https://www.udesc.br/bu/manuais/ficha

Tenfen, Rafael
Caracterização da Evolução do Uso de Protocolos em Ataques DRDoS com Base em Dados de Honeypots / Rafael Tenfen. - Joinville, 2023.
63 p. : il. ; 30 cm.

Orientador: Dr. Rafael Rodrigues Obelheiro.
.
Dissertação (Mestrado) - Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação em Computação Aplicada, Joinville, 2023.

1. ataque de negação de serviço. 2. DRDoS. 3. *honeypot*. 4. caracterização de tráfego. I. Obelheiro, Dr. Rafael Rodrigues . II. Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação em Computação Aplicada. III. Título.

RAFAEL TENFEN

CARACTERIZAÇÃO DA EVOLUÇÃO DO USO DE PROTOCOLOS EM ATAQUES DRDOS COM BASE EM DADOS DE HONEYPOTS

Dissertação apresentada ao Programa de Pós–Graduação em Computação Aplicada do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina, como requisito parcial para a obtenção do grau de Mestre em Computação Aplicada.

Orientador: Dr. Rafael Rodrigues Obelheiro

BANCA EXAMINADORA:

Dr. Rafael Rodrigues Obelheiro
CCT/UDESC

Membros:

Dr. Rafael Rodrigues Obelheiro
Nome da Instituição

Dr. Ricardo Jose Pfitscher
UFSC

Dr. Charles Christian Miers
CCT/UDESC

Joinville, 31 de janeiro de 2023

Este trabalho é dedicado aos desenvolvedores
que buscam conhecimento além do trabalho.

AGRADECIMENTOS

À minha família, em especial minha mãe Marlete da Silva, minha avó Darci de Almeida Coelho, meu pai Nelson Luís Tenfen que me ajudaram durante essa caminhada.

Aos meus sogros Márcio Esser e Lurdes Wippel Esser e sem dúvidas a minha namorada Beatriz Wippel Esser, que me incentivaram a crescer profissionalmente e finalizar a pós-graduação.

À Fundação Universidade do Estado de Santa Catarina (UDESC) e o seu colegiado em geral, mas principalmente ao meu orientador Prof. Dr. Rafael Rodrigues Obelheiro pela orientação e estar presente para auxiliar em todos os desafios dessa pós-graduação. Ao M.Sc. Tiago Heinrich por todas as dicas e sugestões que fizeram a diferença na implementação desse trabalho.

Por fim, ao apoio da Fundação de Amparo à Pesquisa e Inovação do Estado de Santa Catarina (FAPESC)[1].

[1] <https://fapesc.sc.gov.br/>

"Wikipedia is the best thing ever.
Anyone in the world can write
anything they want about any
subject so you know you are
getting the best possible
information."
(Michael Gary Scott, The Office,
Season 3: The Negotiation)

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 coletar dados que os atacantes enviam para vítimas através das requisições. Um bom entendimento do tráfego de ataque permite aperfeiçoar mecanismos de monitoramento e defesa. Neste trabalho, dados coletados por um *honeypot* são usados para caracterizar a evolução de ataques DRDoS envolvendo nove protocolos baseados em UDP durante 1278 dias (3,6 anos), ao longo dos quais foram observados 7,6 milhões de ataques contra 1,4 milhões de vítimas distintas. A pesquisa destaca evoluções no tráfego de ataque, como uma mudança de ênfase em Chargen e Memcached para CLDAP, e analisa os *payloads* das requisições de ataque ao longo do tempo, mostrando que estes permanecem basicamente inalterados, com algumas exceções.

Palavras-chave: ataque de negação de serviço, DRDoS, *honeypot*, caracterização de tráfego.

ABSTRACT

Distributed reflection denial-of-service (DRDoS) attacks are 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 request that the attackers sent to the victims. A good understanding of attack traffic enables us to enhance mitigation and monitoring capabilities. In this paper, we use honeypot data to characterize the evolution of DRDoS attacks involving nine UDP-based protocols over 1278 days (3.6 years), during which we observed 7.6 million attacks against 1.4 million unique victims. We highlight the evolution of attack traffic, such as a shift from Chargen and Memcached towards CLDAP, and analyze attack payloads over time, showing that they remain mostly unchanged, apart from a few exceptions.

Keywords: distributed reflection denial-of-service attacks, DRDoS, honeypots, traffic characterization.

LISTA DE ILUSTRAÇÕES

Figura 1 – Estratégia de ataques distribuído de negação de serviço por reflexão. 16
Figura 2 – Anatomia de um ataque DDoS. 19
Figura 3 – Anatomia de um ataque DRDoS. 23
Figura 4 – Ataques e requisições por trimestre. Observar escalas diferentes no eixo *y*. . 36
Figura 5 – Novas vítimas por trimestre. 37
Figura 6 – Vítimas novas e distintas por trimestre. 38
Figura 7 – Ataques e requisições do Chargen. Observar escalas diferentes no eixo *y*. . . 39
Figura 8 – Ataques e requisições do CLDAP. Observar escalas diferentes no eixo *y*. . . 40
Figura 9 – Ataques e requisições do DNS. Observar escalas diferentes no eixo *y*. 41
Figura 10 – Ataques e requisições do Memcached. Observar escalas diferentes no eixo *y*. 41
Figura 11 – Ataques e requisições do QOTD. Observar escalas diferentes no eixo *y*. . . . 42
Figura 12 – Ataques e requisições do SSDP. Observar escalas diferentes no eixo *y*. . . . 43
Figura 13 – Evolução temporal das requisições por protocolo. 43
Figura 14 – Chargen e QOTD – porcentagem de requisições até 2 bytes. 45
Figura 15 – CLDAP e SSDP – *payloads* predominantes por trimestre. 46
Figura 16 – CoAP – principais *payloads* por trimestre. 46
Figura 17 – Incidência de `MONLIST` em ataques usando NTP. 47
Figura 18 – Requisições DNS por QTYPE. 48
Figura 19 – Longevidade de RRs em ataques DNS. 49
Figura 20 – Relação de ataques e comandos Memcached. 51

LISTA DE TABELAS

Tabela 1 – Linha temporal de ataques de negação de serviço. 20
Tabela 2 – Visão geral dos protocolos utilizados em ataques DRDoS. 24
Tabela 3 – Resumo dos trabalhos relacionados. 31
Tabela 4 – Requisições e ataques observados pelo *honeypot*. 35
Tabela 5 – Observações por ano. Os anos marcados com * são incompletos. 35
Tabela 6 – Caracterização dos protocolos implementados pelo MP-H. 44
Tabela 7 – Top 10 RRs com maior longevidade. 49
Tabela 8 – RRs populares em estudos anteriores. 50
Tabela 9 – Repetições de TxID em ataques DNS. 50

LISTA DE ABREVIATURAS E SIGLAS

Chargen	Character Generator Protocol
CLDAP	Connection-less Lightweight Directory Access Protocol
CoAP	Constrained Application Protocol
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DRDoS	Distributed Reflection Denial-of-Service
Gbps	Gigabits por segundo
HCF	Hop Count Filtering
HTTP	Hypertext Transfer Protocol
LDAP	Lightweight Directory Access Protocol
ICMP	Internet Control Message Protocol
IoT	Internet of things
IP	Internet Protocol
mDNS	Multicast DNS
NAT	Network Address Translation
NTP	Network Time Protocol
PLATO	Programmed Logic for Automatic Teaching Operations
QOTD	Quote of the Day
RFC	Request for Comments
RIP	Routing Information Protocol
RPC	Remote Procedure Call
RR	Resource Record
SSDP	Simple Service Discovery Protocol
SNMP	Simple Network Management Protocol
Tbps	Terabytes por segundo
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TxID	Transaction ID

UDP	User Datagram Protocol

SUMÁRIO

1 INTRODUÇÃO 14
1.1 OBJETIVOS E MÉTODO DE PESQUISA 16
1.2 ESTRUTURA DO DOCUMENTO 17
2 FUNDAMENTAÇÃO TEÓRICA 18
2.1 ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO (DDOS) 18
2.2 ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO POR REFLEXÃO (DRDOS) 21
2.3 HONEYPOTS 26
2.4 CONSIDERAÇÕES DO CAPÍTULO 27
3 PROPOSTA 29
3.1 TRABALHOS RELACIONADOS 29
3.2 DEFINIÇÃO DO PROBLEMA 31
3.3 PROPOSTA 32
3.4 CONSIDERAÇÕES DO CAPÍTULO 32
4 COLETA E ANÁLISE DE DADOS 33
4.1 COLETA DE DADOS 33
4.2 DEFINIÇÕES ADOTADAS 34
4.3 OBSERVAÇÕES GERAIS 34
4.4 OBSERVAÇÕES POR PROTOCOLO 38
4.5 ANÁLISE DE PAYLOADS 44
4.6 DISCUSSÃO DOS RESULTADOS 51
4.7 CONSIDERAÇÕES DO CAPÍTULO 53
5 CONCLUSÃO 54
REFERÊNCIAS 56

1 INTRODUÇÃO

Negação de serviço (*denial-of-service*, DoS), é uma técnica pela qual um atacante utiliza um equipamento conectado à rede para tirar de operação um serviço, um computador ou uma rede conectada à Internet (CERT.BR, 2016). Ataques de negação de serviço podem ter diversas motivações, como motivos pessoais, ganho material, financeiro, político ou puramente destrutivo (MIRKOVIC; REIHER, 2004; ROSSOW, 2014; GUPTA; BADVE, 2017). Tais ataques interrompem o funcionamento de serviços, ou os tornam demasiadamente lentos, induzindo sobrecargas, seja por excesso de requisições (ataques volumétricos) ou usando requisições malformadas que exploram vulnerabilidades das vítimas (ataques semânticos) (MIRKOVIC; REIHER, 2004). Em ataques volumétricos, como servidores, equipamentos de rede e enlaces possuem recursos computacionais finitos, ao enviar mais requisições do que um elemento é capaz de processar 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 simultaneamente no ataque, ele 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 dando uma contribuição para o ataque. Se o número de dispositivos for suficientemente grande, a contribuição de cada um pode ser relativamente pequena (THOMAS; CLAYTON; BERESFORD, 2017); por exemplo, é possível produzir um ataque de 100 Gbps com 100 mil dispositivos gerando 1 Mbps (ou 125 KB/s) de tráfego cada.

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 de dispositivos infectados por *malware* que podem ser remotamente controlados 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 tráfego de ataque do tráfego legítimo tendo em vista a variedade de fontes de tráfego e o volume de dados que cada uma contribui para o ataque (WELZEL; ROSSOW; BOS, 2014).

Os ataques DDoS continuam a se tornar cada vez mais devastadores. Em agosto de 2021, a Microsoft registrou um ataque de 2,4 Tbps contra a Azure Cloud Service (RANGAPUR; KANAKAM; JUBILSON, 2022), três meses depois em outro recorde para a Microsoft com um ataque de 3,47 Tbps a uma taxa de 340 milhões de pacotes por segundo (TOH, 2022). Já em junho de 2022 a Google Cloud registrou o ataque com a maior taxa de requisições por segundo, atingindo um pico de 46 milhões de requisições por segundo (KINER; KONDURU, 2022).

Atacantes podem incrementar seus ataques estruturando-os para utilizarem refletores.

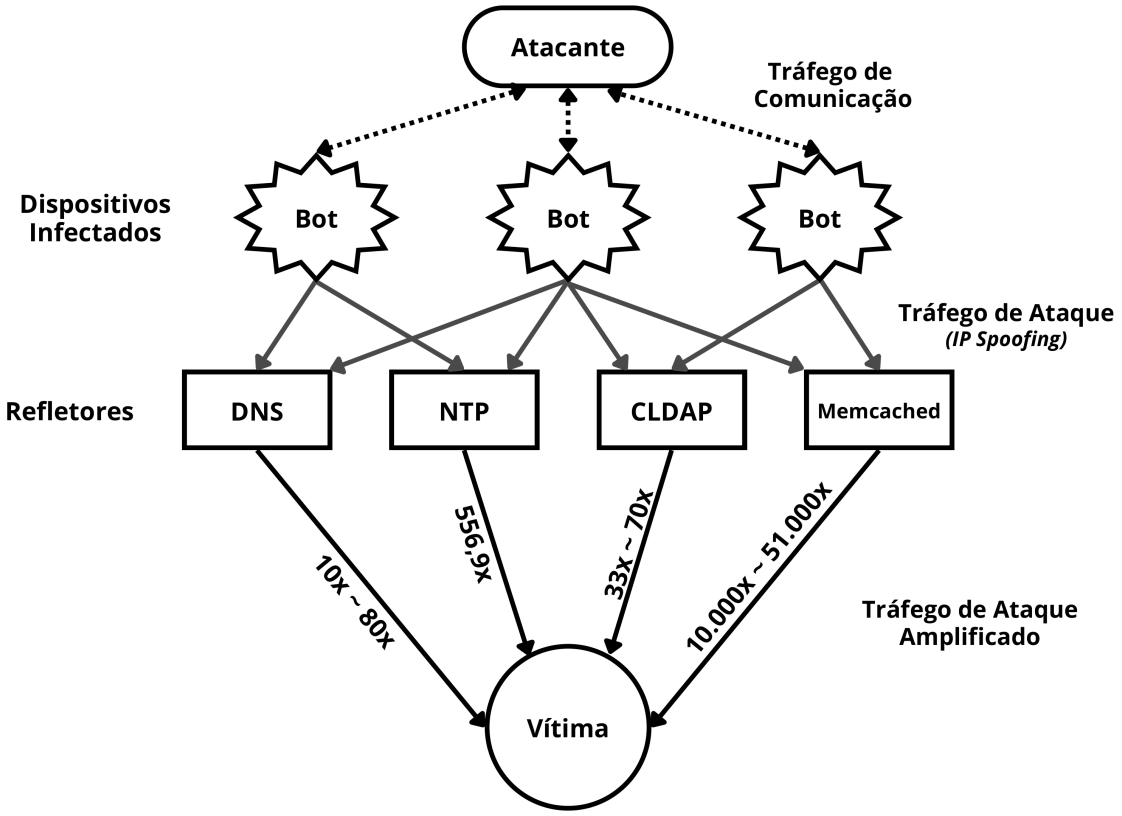
Um refletor é qualquer nó em uma rede que envia uma resposta a um pacote recebido (PAXSON, 2001). Assim, por exemplo, servidores Web, servidores DNS (*Domain Name System*) e roteadores são refletores. A reflexão propriamente dita ocorre quando requisições têm o endereço de origem forjado como sendo o de uma vítima, o que faz com que os refletores respondam para a vítima, e não para quem enviou as requisições. Refletores amplificam a quantidade de dados enviados quando as respostas contêm mais bytes ou pacotes (ou ambos) do que as requisições correspondentes. 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).

A Figura 1 apresenta, de modo simplificado, o fluxo de funcionamento de um ataque DRDoS. O atacante controla os *bots*, que são os dispositivos infectados com um *malware*, instruindo-os a enviarem requisições para um ou mais refletores utilizando o endereço de (*Internet Protocol*, IP) do alvo (vítima) como endereço de origem, levando os refletores a acreditarem que a origem das requisições é a vítima, e assim enviarem as respostas para esta. A amplificação obtida no ataque varia, pois as respostas podem ter de 5,5 até 51.000 vezes a quantidade de bytes enviada pelos dispositivos infectados, dependendo do protocolo (HEINRICH, 2019). Uma vítima não tem dificuldade para identificar os refletores, que correspondem aos endereços de origem nos pacotes do ataque. Já o operador de um refletor não consegue localizar facilmente o dispositivo infectado que está enviando requisições ao refletor, pois endereço de origem que aparece no tráfego de ataque é o da vítima (PAXSON, 2001).

Uma forma de observar ataques é usando *honeypots*, que são recursos computacionais abertos dedicados a serem sondados, atacados ou comprometidos (HOEPERS; STEDING-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. Para observar especificamente ataques DRDoS, podem ser usados *honeypots* que imitem o comportamento de refletores (ROSSOW, 2014; KRÄMER et al., 2015; HEINRICH, 2019). Se a rede de um *honeypot* é monitorada 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 observação 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 (ROSSOW, 2014; KRÄMER et al., 2015; THOMAS; CLAYTON; BERESFORD, 2017; HEINRICH; LONGO; OBELHEIRO, 2017; HEINRICH; OBELHEIRO, 2019; HEINRICH; OBELHEIRO; MAZIERO, 2021). 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 quais são as vítimas mais afetadas. Alguns trabalhos, como (THOMAS; CLAYTON; BERESFORD, 2017; HEINRICH; LONGO; OBELHEIRO, 2017; HEINRICH; OBELHEIRO; MAZIERO, 2021), também realizam uma análise dos *payloads*

Figura 1 – Estratégia de ataques distribuído de negação de serviço por reflexão.



Fonte: Autor (2023)

usados nos ataques de reflexão. No entanto, mesmo com dados coletados por longos períodos (por exemplo, 1010 dias em (THOMAS; CLAYTON; BERESFORD, 2017)), a evolução temporal do tráfego, e particularmente dos *payloads* usados, é pouco explorada.

Este trabalho de mestrado preenche esta lacuna. São analisados dados de ataques DRDoS envolvendo nove protocolos (*Character Generator Protocol*, Chargen), (*Connection-less Lightweight Directory Access Protocol*, CLDAP), (*Constrained Application Protocol*, CoAP), DNS, Memcached, (*Network Time Protocol*, NTP), (*Quote of the Day*, QOTD), (*Simple Service Discovery Protocol*, SSDP) e Steam), coletados por um *honeypot* MP-H (HEINRICH, 2019) ao longo de 1278 dias, com vistas a descrever o tráfego observado e, principalmente, entender a evolução temporal dos ataques e dos *payloads*.

1.1 OBJETIVOS E MÉTODO DE PESQUISA

O objetivo geral desta dissertação de mestrado é analisar a evolução do tráfego DRDoS observado por um *honeypot* MP-H que foi implantado em 2018. Este objetivo geral pode ser desdobrado nos seguintes objetivos específicos:

1. Compreender a dinâmica de ataques DRDoS usando os protocolos implementados pelo

honeypot;

2. Analisar estatísticas gerais do tráfego capturado;
3. Estudar a evolução do tráfego observado pelo *honeypot* durante o período de coleta;
4. Analisar a evolução temporal dos *payloads* usados em ataques DRDoS.

Esta pesquisa deu seguimento ao trabalho de (HEINRICH, 2019), que introduziu o *honeypot* MP-H e colocou sua primeira instância em operação.

Este trabalho adota os métodos de pesquisa referenciada para a revisão bibliográfica, e de estudo observacional longitudinal (considerando o *honeypot* como instrumento de medida) para a coleta e análise de dados.

1.2 ESTRUTURA DO DOCUMENTO

Esse documento está organizado em cinco capítulos. O Capítulo 2 apresenta a fundamentação teórica necessária para o entendimento do trabalho. O Capítulo 3 discorrem a revisão e discussão de trabalhos relacionados, assim como o detalhamento da proposta. O Capítulo 4 descreve o *honeypot* MP-H, as definições adotadas, detalha a coleta e análise dos dados e discute os resultados. O Capítulo 5 apresenta as considerações finais e perspectivas futuras da pesquisa.

2 FUNDAMENTAÇÃO TEÓRICA

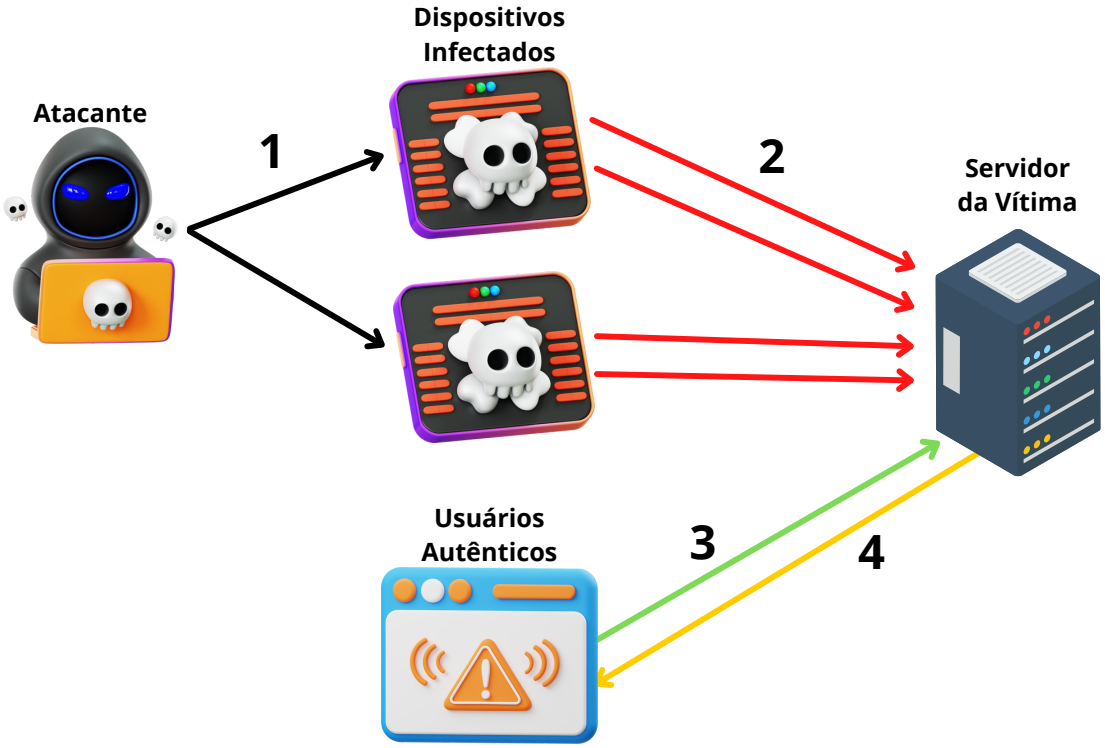
Este capítulo faz uma fundamentação dos conceitos necessários ao entendimento deste trabalho baseado na literatura já existente. A Seção 2.1 expõe definições e fundamentos de ataques DDoS. A Seção 2.2 apresenta fundamentos de ataques DRDoS e os principais protocolos utilizados nesse trabalho. A Seção 2.3 aborda conceitos e funcionalidades de *honeypots*. Por fim a Seção 2.4 apresenta as considerações do capítulo.

2.1 ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO (DDOS)

O objetivo de um ataque de negação de serviço (*Denial of Service*, DoS) é prejudicar o uso legítimo de um recurso computacional, como um servidor ou um enlace de rede, tornando-o indisponível ou excessivamente lento (SHIREY, 2007). 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. 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 são externos ao próprio sistema ou rede da vítima. Em muitos casos, ataques provêm de 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).

Um ataque distribuído de negação de serviço DDoS usa vários hospedeiros na Internet para enviar tráfego para uma vítima de forma coordenada (NAZARIO, 2008). Conforme apresentado de modo simplificado na Figura 2, após infectar dispositivos com um *malware* que permite o controle de modo remoto, um atacante envia comandos representados pela seta em preto (1) para que os dispositivos infectados enviem tráfego de ataque para uma ou mais vítimas representadas pelas setas em vermelho (2). Além das requisições realizadas pelos dispositivos infectados, o servidor da vítima recebe também requisições de seus usuários autênticos representadas pela seta na cor verde (3), e assim, ao receber mais requisições do que consegue processar, o servidor da vítima sofre a saturação de seus recursos computacionais e não consegue responder a todas as requisições, negando serviço aos seus usuários autênticos representado pela seta em amarelo (4).

Figura 2 – Anatomia de um ataque DDoS.



Fonte: Autor (2023)

Os ataques DDoS estão em constante evolução, pois a natureza da tecnologia usada e as motivações dos atacantes estão mudando (NAZARIO, 2008). A Tabela 1 apresenta uma linha do tempo que ilustra a dimensão e a evolução de ataques DoS ao longo do tempo. O crescimento exponencial em todas as métricas é aparente, muitas vezes gerando manchetes alarmistas à medida que os volumes de ataque aumentam, mas é preciso levar em consideração o crescimento exponencial da própria Internet, que também aumenta constantemente e fornece largura de banda e computação aos defensores (MENSCHER, 2020).

O projeto da Internet tem seu foco na eficiência de movimentação de pacotes da origem para o destino, esse projeto segue o paradigma fim a fim, em que a rede intermediária fornece o serviço de encaminhamento de pacotes com semântica de melhor esforço (*best-effort*), 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 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

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 PLATO (DEAR, 2010).
1988	Robert Morris foi o responsável por paralisar grande parte da Internet através de um *malware* conhecido como *worm* (WOODY; MEAD; SHOEMAKER, 2012).
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 uma conferência que derrubou o serviço de Internet de um grande hotel de Las Vegas por mais de uma hora (MEHRDAD et al., 2018).
1998	Foi realizado o primeiro ataque de reflexão conhecido como ataque *smurf*, que explorava 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 foram emitidos alertas sobre a possibilidade de utilizar o DNS para a realização de ataques DDoS (NIST, 1999; CERT/TCC, 1999).
2003	O primeiro *flash worm*, chamado Slammer, infectou 75 milhões de hospedeiros em dez minutos e alcançou 80 milhões de pacotes por segundo (MOORE et al., 2003).
2009	O *worm* MyDoom foi reaproveitado para infectar 50 mil hospedeiros e realizar um ataque que alcançou picos de 13 Gbps (ZETTER, 2009).
2012	Crescimento nos ataques DRDoS explorando DNS, Chargen, NTP e (*Simple Network Management Protocol*, SNMP) (PROLEXIC, 2013b).
2013	30.000 servidores DNS foram usados em um ataque contra a Spamhaus que atingiu picos de 300 Gbps (PRINCE, 2013). Outros ataques realizados 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) foram explorados para realizar ataques que alcançaram $\approx$ 1 Tbps de tráfego (a maior parte do tráfego foi gerado por câmeras de circuito fechado ligadas à Internet) (KHANDELWAL, 2016).
2017	Em setembro, a Google Cloud registrou o maior ataque até então, chegando a 2,5 Tbps de tráfego e abusando mais de 180 mil refletores utilizando protocolos como CLDAP, DNS e SNMP (MENSCHER, 2020).
2018	Atacantes exploraram servidores 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 1,4 Tbps de tráfego (NEWMAN, 2018). Uma semana depois deste ataque, a NETSCOUT (BIENKOWSKI, 2018) registrou um ataque de 1,7 Tbps de tráfego.
2020	No primeiro trimestre, ataques utilizando o protocolo CLDAP atingiram um volume de 2,3 Tbps de tráfego (SHIELD, 2020). Em outubro, a bolsa de valores da Nova Zelândia foi alvo de ataques DDoS que duraram 4 dias, causando a parada de compra e venda de ações múltiplas vezes (NETSCOUT, 2020).
2021	Nas primeiras semanas de janeiro de 2021, os ataques DRDoS contra organizações tornaram-se cada vez mais contínuos (HAQUE et al., 2022). Além disso, (NETSCOUT, 2021) registrou cerca de 5,4 milhões de ataques DDoS.
2022	Ataques com inundações de tráfego acima de 1 Tbps tornaram-se comuns (KHANTIMIROV, 2022). Em maio de 2022, a Radware mitigou um ataque que utilizava *carpet bombing*, e que chegou a um volume total de 2,9 petabytes de dados (LOHRMANN, 2022).

Fonte: Adaptado de (HEINRICH, 2019)

spoofing e a possibilidade de ataques DDoS (MIRKOVIC; REIHER, 2004).

A técnica de IP *spoofing* consiste em falsificar o endereço IP de origem de um pacote usando um endereço arbitrário ou que corresponde ao endereço IP de outro dispositivo (FERGUSON; SENIE, 2000). Essa técnica é frequentemente usada em ataques DoS para mascarar os endereços de origem dos atacantes e dificultar ainda mais a sua identificação. Como o endereço de origem de um pacote IP é usado como endereço de destino para o tráfego de resposta, sua falsificação faz com que esse tráfego de resposta seja encaminhado para outro nó da rede, e não para a real origem. Como muitos ataques DoS exigem apenas que a vítima receba um grande volume de tráfego (ou seja, o atacante não tem interesse no tráfego de resposta), eles não são prejudicados pelo envio do tráfego de resposta para outro destino; na verdade, o atacante pode preferir não receber as respostas para evitar saturar os seus próprios recursos. O IP *spoofing* pode ser combatido com os métodos apresentados pela BCP 38 (FERGUSON; SENIE, 2000), que preconizam que um provedor de acesso à Internet bloqueie tráfego com endereços IP de origem que não pertençam à sua rede, evitando que esse tráfego chegue em outras redes. É importante destacar que esse método de defesa evita que pacotes com endereços de origem forjados saiam da rede do provedor (ou nela circulem, dependendo do ponto de filtragem), mas não impede que essa rede receba tráfego com endereços forjados de seus clientes ou de outros provedores. Portanto, o combate ao IP *spoofing* requer que a BCP 38 seja adotada no maior número possível de redes que compõem a Internet.

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

Ataques distribuídos de negação de serviço por reflexão (*Distributed Reflection Denial of Service*, DRDoS), são ataques DDoS em que o tráfego não é enviado diretamente dos hospedeiros comprometidos (também chamados de *bots*) para a vítima, mas encaminhado por intermediários conhecidos como refletores. 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. Um refletor é qualquer hospedeiro IP que responde a um pacote recebido (PAXSON, 2001). Exemplos comuns de refletores são servidores UDP (*User Datagram Protocol*) que respondem a requisições sem verificar o endereço IP do remetente (ROSSOW, 2014). Frequentemente, essas respostas são maiores que as requisições correspondentes. Isso promove a amplificação do tráfego de ataque: o refletor recebe requisições a uma taxa de b bits por segundo e produz respostas a uma taxa de $F \cdot b$ bits por segundo, onde o fator de amplificação F é dado pela razão entre o tamanho das respostas e o tamanho das requisições (ROSSOW, 2014). Um servidor que é utilizado como refletor pode implementar vários protocolos utilizando o mesmo endereço IP, mapeando apenas a porta de destino da requisição para definir o protocolo que irá utilizar. 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).

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

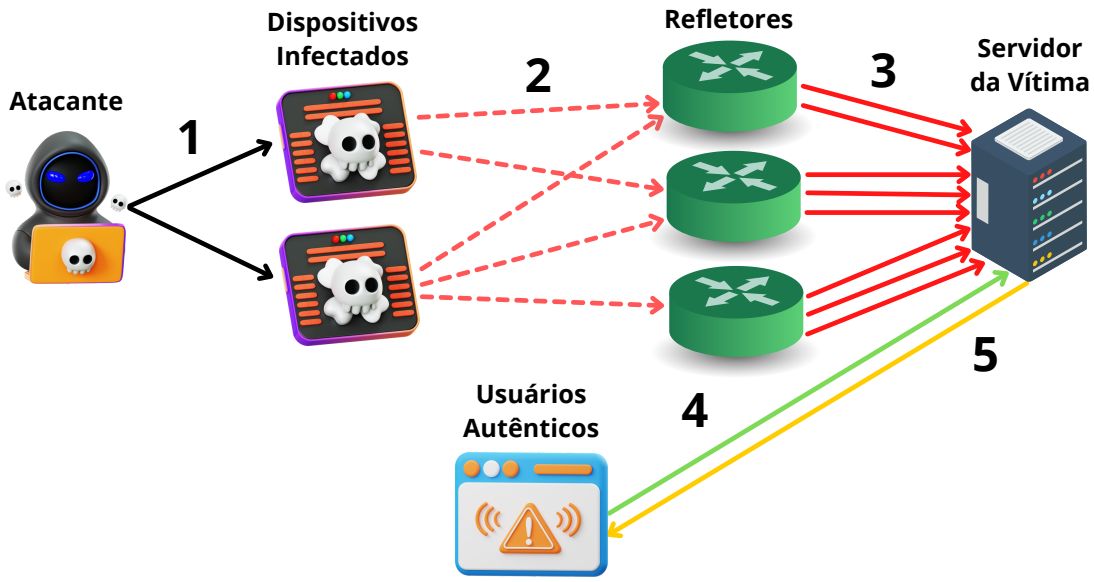
1. Disfarçar sua identidade, pois as vítimas recebem tráfego de amplificadores, ou seja, sistemas que podem ser abusados para enviar tráfego para a vítima em nome do atacante;
2. O abuso simultâneo de múltiplos amplificadores permite que um ataque DoS altamente distribuído seja conduzido a partir de um único *uplink* na Internet; e
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.

A Figura 3 apresenta de modo simplificado o esquema de um ataque DRDoS. Um atacante que controle dispositivos infectados envia comandos representados pelas setas em preto (1) para que esses dispositivos enviem tráfego de ataque para os refletores representados pelas setas tracejadas em vermelho (2). Como o tráfego de ataque usa IP *spoofing*, os refletores enviam o tráfego de resposta (potencialmente amplificado) para a vítima, como mostram as setas em vermelho (3). Enquanto o ataque acontece, usuários autênticos também enviam requisições para a vítima, como representado pela seta na cor verde (4). Contudo, o servidor da vítima possui recursos finitos de processamento, sofrendo saturação ao receber mais tráfego do que consegue processar, e não conseguindo responder aos seus usuários legítimos, como representado pela seta em amarelo (5).

Ataques DRDoS são complexos de serem solucionados, pois a vítima nem sequer realiza solicitações para os refletores e recebe uma inundação de tráfego. Além disso, com a técnica de IP *spoofing* existe o problema para rastrear os *bots* que estão enviando requisições com IP forjado e que de forma não rara pode envolver mais de uma camada de nós, tipicamente em redes e jurisdições distintas para conseguir rastrear o atacante que envia os comandos (HEINRICH, 2019). Já no lado do operador de um refletor, também é difícil localizar o dispositivo infectado que está bombardeando o refletor, pois o tráfego enviado ao refletor não possui o endereço de origem do *bot*, mas sim o endereço de origem da vítima (PAXSON, 2001).

Apesar das dificuldades, alguns trabalhos na literatura abordam técnicas de mitigação de ataques DRDoS. Backes et al. (2016) apresenta um mecanismo de defesa de filtragem da contagem de saltos (*Hop Count Filtering*, HCF); Paxson (2001) argumenta que o tráfego gerado pelos refletores pode ter uma regularidade semântica suficiente para ser filtrado próximo à vítima; Nawrocki et al. (2019) aponta o uso de *blackholing*; o uso de serviços externos de proteção que realizam inspeção e filtragem de tráfego de ataque (*traffic scrubbing*) (MOURA et al., 2020); e a RFC 5358 (DAMAS; NEVES, 2008) apresenta diretrizes de configuração para evitar que servidores sejam abusados como refletores.

Figura 3 – Anatomia de um ataque DRDoS.



Fonte: Autor (2023)

Protocolos utilizados em DRDoS

A Tabela 2 apresenta um resumo de 18 protocolos empregados em ataques DRDoS; os protocolos estão ordenados de modo decrescente pelo seu fator de amplificação. A maioria consiste em protocolos de aplicação baseados em UDP (ROSSOW, 2014). O presente trabalho analisa dados coletados sobre nove desses protocolos, que são aqueles implementados pelo *honeypot* utilizado para a coleta dos dados: Chargen, CLDAP, CoAP, DNS, Memcached, NTP, QOTD, SSDP e Steam. Todos eles usam o UDP como protocolo de transporte. A função desses protocolos e a forma como eles são explorados em ataques DRDoS são discutidas a seguir.

O Memcached (MEMCACHED, 2022) é um sistema de armazenamento chave-valor usado majoritariamente como *cache* de objetos e conteúdo dinâmico de páginas web, que pode usar tanto UDP quanto (*Transmission Control Protocol*, TCP) como protocolo de transporte. Em ataques DRDoS, o Memcached é explorado basicamente de duas formas (NEWMAN, 2018):

1. Usando o comando `stats` para solicitar estatísticas do sistema, o que produz uma mensagem com cerca de 1,3 KB; e

2. Usando inicialmente o comando `set` para atribuir um valor a uma chave, e depois consultando essa chave repetidamente usando o comando `get` – caso o valor seja grande

Tabela 2 – Visão geral dos protocolos utilizados em ataques DRDoS.

Protocolo	**Referência**	**Fator de Amplificação**
Memcached	(NEWMAN, 2018)	10.000–51.000
NTP	(CZYZ et al., 2014)	556,9
Chargen	(ROSSOW, 2014)	358,8
QOTD	(CISA, 2019)	140,3
RIP	(AKAMAI, 2016)	131,24
Half-life	(NOLLA, 2013)	109,8
HTTP	(BECKETT; SEZER, 2017)	79–100
CoAP	(UTECH; OBELHEIRO, 2020; ASERT, 2019)	25–34
CLDAP	(ARTEAGA; MEJIA, 2017)	33–70
Quake 3	(ROSSOW, 2014)	63,9
TFTP	(SIEKLIK; MACFARLANE; BUCHANAN, 2016)	60
LDAP	(CISA, 2019)	46–55
DNSSEC	(RIJSWIJK-DEIJ; SPEROTTO; PRAS, 2014)	40–55
DNS	(HOEPERS et al., 2016)	28–54
SSDP	(MAJKOWSKI, 2017)	30,8
Sun RPC	(SUBRAMANI; PERDISCI; KONTE, 2021)	7–28
SNMP	(PROLEXIC, 2013a; GROUP et al., 2012)	6,3
Steam	(CISA, 2019; NOLLA, 2013)	5,5
BitTorrent	(ROSSOW, 2014)	3,8
ICMP	(CERT, 1998; KUMAR, 2007)	não disponível

Fonte: Adaptado de (HEINRICH, 2019)

(na configuração padrão, valores podem ter até 1 MB de tamanho), é possível obter uma amplificação significativa.

O NTP (*Network Time Protocol*) (MILLS et al., 2010) é um protocolo usado para sincronizar relógios através da rede. Embora requisições de sincronização gerem respostas pequenas (ou seja, com pouca amplificação de tráfego), o NTP também suporta mensagens de controle, que podem gerar uma maior amplificação. Dentre essas mensagens, destaca-se o comando `MONLIST`, que retorna uma lista com até 600 nós que usaram recentemente o servidor contactado (HABERMAN, 2019); como requisições `MONLIST` são pequenas (da ordem de 64 bytes), isso pode gerar um fator de amplificação superior a 550 (CZYZ et al., 2014).

Chargen (POSTEL, 1983a) e *Quote of the Day* (QOTD) (POSTEL, 1983b) são serviços desenvolvidos com o objetivo de auxiliar na depuração de problemas de rede. O Chargen, ao receber um pacote, gera uma resposta contendo de 0 a 512 caracteres aleatórios, desprezando o conteúdo da requisição (POSTEL, 1983a). O QOTD, por sua vez, envia uma citação com até 512 caracteres imprimíveis, cujo conteúdo não é padronizado (POSTEL, 1983b). Embora as respostas tenham conteúdo limitado a 512 bytes, os protocolos são suscetíveis a amplificação significativa de tráfego, uma vez que mesmo requisições contendo zero bytes de *payload* são suficientes para gerar respostas. Mesmo sendo protocolos legados e pouco usados para o seu

propósito original, ainda é possível encontrar um grande número de refletores Chargen e QOTD na Internet (KARAMI; PARK; MCCOY, 2016).

O CoAP (*Constrained Application Protocol*) (SHELBY; HARTKE; BORMANN, 2014) é um protocolo de aplicação semelhante ao HTTP (*Hypertext Transfer Protocol*) (FIELDING et al., 1999) voltado para comunicação entre dispositivos de capacidade limitada, notadamente no contexto da Internet das Coisas (*Internet of Things*, IoT). Uma requisição CoAP contém uma operação (como `GET` ou `POST`) e uma URI (*Universal Resource Identifier*) que identifica o *endpoint* (recurso) sobre o qual será realizada a operação. Ataques DRDoS usando o CoAP geralmente exploram a URI `.well-known/core`, que retorna uma mensagem de centenas de bytes contendo uma lista de informações sobre os serviços disponíveis no servidor (ASERT, 2019).

O CLDAP (*Connection-less Lightweight Directory Access Protocol*) (YOUNG, 1995) é um serviço de diretórios, usado tipicamente em redes Windows por servidores *Active Directory*. Ataques DRDoS usando CLDAP geralmente exploram requisições `NETLOGON` que solicitam uma lista de atributos suportados por um servidor, conseguindo assim um fator de amplificação de até 70 vezes (ARTEAGA; MEJIA, 2017).

O DNS (*Domain Name System*) é o sistema distribuído de resolução de nomes adotado na Internet (MOCKAPETRIS, 1987a; MOCKAPETRIS, 1987b). Sua função mais conhecida é traduzir nomes de hospedeiros, como `www.example.org`, em endereços IP, como 192.0.2.1. O DNS possui um espaço de nomes hierárquico, organizado em forma de árvore. Cada nó da árvore, ou registro de recurso (*resource record*, RR), possui três atributos fixos: nome (QNAME), tipo (QTYPE) e classe (QCLASS). Na Internet, a classe dos RRs geralmente é `IN` (na sequência da discussão, fica subentendido que os RRs pertencem a essa classe). Um RR também contém um item de dados (RDATA), que pode ser simples ou composto, com formato dependendo do tipo. Por exemplo, um RR do tipo `A` tem um item de dados simples, que representa um endereço IP, enquanto um RR do tipo `MX`, que representa um servidor de email para um domínio, possui um item de dados composto, formado por um nome DNS e uma preferência numérica. Pela característica dos seus dados, o DNS é naturalmente suscetível a amplificação: uma consulta DNS especifica os atributos de um RR (QNAME, QTYPE, QCLASS) e pode gerar como resultado o RR completo (atributos mais RDATA) ou mesmo um conjunto de RRs (incluindo RDATA).

Existem dois tipos básicos de servidores DNS: servidores com autoridade e servidores recursivos (HOFFMAN; SULLIVAN; FUJIWARA, 2019). Um servidor com autoridade é responsável pelos dados (RRs) de uma ou mais sub-árvores do espaço de nomes, ou domínios. Tais servidores devem responder a consultas referentes aos domínios sob sua autoridade, independente da origem dessas consultas, que podem ser clientes ou outros servidores DNS. Já um servidor recursivo é usado por clientes DNS para resolver nomes independentemente de domínio; para isso, o recursivo contacta os servidores com autoridade pertinentes.

Um servidor recursivo deve atender a uma população definida de clientes DNS (por exemplo, um provedor Internet geralmente possui servidores DNS recursivos que são usados

apenas pelos clientes desse provedor). Servidores recursivos que não restringem o acesso à sua população alvo são chamados de recursivos (ou resolvedores) abertos.

Servidores DNS recursivos abertos são usados como refletores em ataques DRDoS (HOEPERS et al., 2016). Os ataques usam consultas com fator de amplificação elevado, podendo chegar a 100x (HEINRICH; LONGO; OBELHEIRO, 2017). Uma funcionalidade do DNS bastante explorada em ataques DRDoS são as consultas tipo `ANY`, que retornam um conjunto de RRs com o QNAME especificado na consulta e qualquer tipo (MOCKAPETRIS, 1987b). Essas consultas, cuja intenção era facilitar a depuração de problemas com o DNS, acabaram sendo aposentadas (declaradas obsoletas) em 2019 justamente em função do seu papel em ataques DRDoS (ABLEY et al., 2019); no entanto, muitos servidores ainda respondem a consultas `ANY`. Outra funcionalidade explorada em ataques DRDoS são as extensões de segurança do DNS (*DNS Security Extensions*, DNSSEC) (RIJSWIJK-DEIJ; SPEROTTO; PRAS, 2014). O DNSSEC introduziu no DNS novos tipos de RRs, com conteúdos que podem chegar a centenas de bytes (ARENDS et al., 2005a). Além disso, o DNSSEC atualizou o algoritmo de processamento de consultas de uma forma que potencializou a amplificação de tráfego (ARENDS et al., 2005b): em um domínio que suporta DNSSEC, uma consulta de 40–50 bytes pode gerar respostas que ultrapassam 4000 bytes (HEINRICH; LONGO; OBELHEIRO, 2017).

O SSDP (*Simple Service Discovery Protocol*) (GOLAND, 1999) fornece um mecanismo de descoberta automática de recursos (como impressoras e telefones celulares) na rede, necessitando de pouca ou nenhuma configuração estática (GOLAND, 1999). Atacantes geralmente usam o comando `M-SEARCH` com as *strings* de busca `upnp:rootdevice` ou `ssdp:all`, que são respondidas pela maior parte dos dispositivos que suportam SSDP, obtendo assim uma amplificação de tráfego de até 30 vezes (MAJKOWSKI, 2017).

O protocolo Steam (VALVE, 2023) é usado por jogos *online* como Counter-Strike, Half-Life e Team Fortress. Com esse protocolo é possível realizar a solicitação de informações de status para inundar uma vítima em potencial com respostas de status do servidor (ROSSOW, 2014; KIM; KIM; KANG, 2016).

Os nove protocolos que são o foco desse trabalho não são os 9 protocolos com maior fator de amplificação, entretanto alguns dos protocolos apresentados na Tabela 2 não fazem sentido estarem disponibilizados por um hospedeiro *honeypot*, como o RIP (*Routing Information Protocol*) que é implementado por roteadores. Por fim, outros protocolos podem vir a ser implementados no futuro pelo *honeypot* para abrangir ainda mais a capacidade de coleta de dados, como por exemplo o protocolo DNSSEC (*Domain Name System Security Extensions*).

2.3 HONEYPOTS

Honeypots são sistemas criados não para serem acessados por usuários legítimos, e sim com o objetivo de serem sondados, atacados ou até mesmo comprometidos (HOEPERS; STEDING-JESSEN; CHAVES, 2007; BHAGAT; ARORA, 2018). A ideia é que *honeypots*

possuam (ou aparentem possuir) vulnerabilidades que possam ser exploradas por atacantes e sejam 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. Geralmente um *honeypot* é um hospedeiro que possui um endereço público na Internet, mas que não oferece nenhum serviço oficial. Por consequência, o hospedeiro 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 um *honeypot* pode ser considerada suspeita (SPITZNER, 2003; HOEPERS; STEDING-JESSEN; CHAVES, 2007).

Honeypots podem ser classificados segundo o nível de interação que oferecem a um atacante (PROVOS; HOLZ, 2007). Um *honeypot* de baixa interatividade 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. Pode-se ainda falar em *honeypots* de média interatividade, que se situam entre esses extremos, tipicamente oferecendo um alto grau de interação para um conjunto limitado de funcionalidades.

No caso de ataques DRDoS, um *honeypot* que se comporte como um refletor pode capturar a interação dos *bots* com os refletores. Múltiplas instâncias de um *honeypot* podem ser utilizadas para recolher dados, e assim permitir a comparação entre os ataques observados pelos diferentes *honeypots*. Dois exemplos de *honeypots* usados para observação de ataques DRDoS são AmpPot (KRÄMER et al., 2015) e MP-H (HEINRICH, 2019).

O MP-H (HEINRICH; OBELHEIRO; MAZIERO, 2021) é um *honeypot* que oferece suporte a nove protocolos diferentes utilizados em ataques DRDoS (Chargen, CLDAP, CoAP, DNS, Memcached, NTP, QOTD, SSDP e Steam). O *honeypot* foi desenvolvido em Python para plataforma Linux, e sua instância original permanece online desde 2018. O MP-H foi projetado para imitar um refletor, recebendo requisições para os vários protocolos e fornecendo respostas que parecem legítimas, registrando todo o tráfego recebido. Uma lista dos ataques que estão ocorrendo (com endereço IP de origem, número de solicitações e carimbos de data/hora da primeira e da última solicitação vistas) é atualizada em tempo real e mantida na memória, sendo periodicamente gravada em armazenamento permanente quando a atividade é baixa. Como não hospeda nenhum serviço anunciado publicamente, uma instância MP-H se tornará um refletor após ser encontrada por meio de varredura. Uma vez descoberto, o endereço do *honeypot* pode ser usado em ataques DRDoS e provavelmente será compartilhado entre os atacantes.

2.4 CONSIDERAÇÕES DO CAPÍTULO

Este capítulo abordou conceitos básicos sobre ataques DDoS e DRDoS, incluindo como diferentes protocolos são usados em ataques por reflexão. Também foi dada uma visão geral

de *honeypots*, como eles podem ser usados para observar ataques DRDoS, e do funcionamento do MP-H, o *honeypot* que foi usado para a coleta de dados neste trabalho. Esses assuntos fundamentam a proposta do trabalho, que será desenvolvida no Capítulo 3.

3 PROPOSTA

Este capítulo apresenta a proposta desta dissertação de mestrado, e está dividido em quatro seções. A Seção 3.1 discute os trabalhos relacionados mais recentes encontrados na literatura. A Seção 3.2 define o problema abordado na dissertação. A Seção 3.3 apresenta a proposta de análise dos dados. A Seção 3.4 traz as considerações do capítulo.

3.1 TRABALHOS RELACIONADOS

Esta seção discute trabalhos correlatos que utilizam, capturam ou analisam *payloads* de ataques DRDoS, que é o foco deste trabalho.

Anagnostopoulos et al. (2013) discutem ataques DRDoS usando os protocolos DNS e DNSSEC. Os autores mostram que servidores DNS mal configurados podem ser explorados e abusados como amplificadores, gerando respostas com tamanhos entre 37 e 44 vezes o tamanho das consultas enviadas pelos atacantes. Contudo, o artigo utiliza o *payload* apenas para mensurar o fator de amplificação, sem examinar outras características.

Rossow (2014) analisou e categorizou ataques DRDoS de 14 protocolos (NTP, SNMP, SSDP, NetBios, Chargen, QOTD, DNS, NetBios, P2P, BitTorrent, Kad, Quake 3, Steam, ZAv2, Sality e Gameover) de dados coletados de modos diferentes, uma das formas foi utilizando um provedor Internet europeu com um milhão de usuários por 12 dias, o outro de duas *darknets* (redes que não abrigam nenhum serviço ou usuário legítimo e que, portanto, não têm por que receber tráfego benigno) durante 28 dias e o por fim um *honeypot* por mais 28 dias, totalizando um período de coleta de 68 dias. Esse trabalho utilizou o *payload* para observar algumas características de requisições exploradas em ataques DRDoS, como o uso de `MONLIST` em ataques NTP e a utilização do QTYPE `ANY` em ataques DNS. Contudo, o trabalho não realiza nenhum tipo de análise temporal.

Krämer et al. (2015) desenvolveram um *honeypot* chamado AmpPot que suporta 10 protocolos (QOTD, Chargen, DNS, NTP, NetBIOS, SNMP, SSDP, MS-SQL e SIP), e que coletou dados durante 121 dias. Foram observados dados de cabeçalho, como os endereços IP de origem e destino, para verificar as regiões geográficas com mais ataques para todos os protocolos. Entretanto, a análise especifica de *payloads* ficou restrita ao DNS, apresentando apenas sobre a longevidade dos registros de recursos (RRs).

Thomas, Clayton e Beresford (2017) utilizaram 65 *honeypots* com suporte a oito protocolos (QOTD, Chargen, DNS, NTP, SSDP, MS-SQL, Portmap e (*Multicast DNS*, mDNS)) para coletar dados por 1010 dias. O trabalho analisa estatisticamente vários aspectos do tráfego observado, e a discussão de *payloads* é restrita aos nomes de domínio mais usados em ataques com o protocolo DNS.

Heinrich (2017) apresentou o DNSpot, um *honeypot* específico para DNS que é um precursor de MP-H. Foi feita uma análise de tráfego capturado pelo DNSpot durante 250 dias. O estudo contemplou tanto dados de cabeçalhos dos pacotes, para mapear a localização geográfica

de origem e destino através dos endereços IP, quanto os *payloads*, para analisar os RRs utilizados em ataques, como os QNAMEs e domínios mais populares. Desse forma, o trabalho contempla uma análise longitudinal com foco em DNS, mas não realiza a avaliação da evolução dos *payloads*.

Heinrich (2019) introduziu o MP-H (inicialmente chamado HReflector), um *honeypot* voltado à observação de ataques DRDoS que coletava tráfego de 7 protocolos (Chargen, DNS, Memcached, NTP, QOTD, SSDP e Steam). O trabalho fez uma análise de tráfego capturado por um período de 255 dias, com foco em ataques multiprotocolo (em que vários protocolos são usados simultaneamente contra uma mesma vítima) e de *carpet bombing* (em que múltiplos endereços IP pertencentes a uma mesma vítima são atacados ao mesmo tempo). Além disso, foram analisados os *payloads* de cada um dos protocolos suportados e a evolução temporal das quantidades de ataques e requisições; a evolução temporal de *payloads* não foi abordada.

Heinrich, Obelheiro e Maziero (2021) usaram o MP-H para capturar e analisar tráfego de ataques DRDoS multiprotocolo e *carpet bombing* durante um período de 731 dias. Além dos protocolos considerados em (HEINRICH, 2019), foram incorporados ao *honeypot* os protocolos CoAP e CLDAP. Embora faça uma análise de *payloads* usados com diferentes protocolos, o trabalho não leva em conta a evolução temporal desses *payloads*.

Kopp, Dietzel e Hohlfeld (2021) analisaram e classificaram tráfego de ataques DDoS para 12 protocolos (CLDAP, DNS, SSDP, Memcached, NTP, RPC, SNMP, Chargen, ARMS, WS-Dis, Device Dis e OpenVPN), utilizando dados observados de um *Internet Exchange Point* (IXP) europeu durante um período de 210 dias. O trabalho teve foco na classificação dos ataques em cada protocolo e também constatou a utilização de ataques multiprotocolo. Além disso, o trabalho observou um pico de 2608 ataques DDoS em apenas um dia de tráfego. Contudo, os *payloads* dos pacotes utilizados nos ataques não foram analisados.

Heinrich et al. (2022) utilizaram quatro instâncias do MP-H para capturar e caracterizar ataques DRDoS durante um período de 1312 dias. O foco do trabalho consiste em analisar as características de tráfego de ataque de acordo com a geolocalização das vítimas, comparando os ataques em diferentes países e continentes.

A Tabela 3 resume os trabalhos relacionados, contrastando-os com o presente trabalho. Constata-se que poucas referências, como (KRÄMER et al., 2015; HEINRICH, 2017; HEINRICH, 2019), focam na análise dos *payloads* utilizados pelos atacantes ou na evolução temporal de algumas características de ataques. No entanto, nenhum dos trabalhos examina como os *payloads* de ataques DRDoS evoluem ao longo do tempo, o que é o diferencial deste trabalho.

Tabela 3 – Resumo dos trabalhos relacionados.

Trabalho	**Protocolos**	**Período**	**Foco de Análise**
(ANAGNOSTOPOULOS et al., 2013)	2 Protocolos	2× ao longo de 6 meses	Visão do atacante e utiliza o *payload* somente para calcular o fator de amplificação.
(ROSSOW, 2014)	14 Protocolos	68 dias	Classificação por protocolo e uso do *payload* a nível de protocolo, sem análise temporal.
(KRÄMER et al., 2015)	10 Protocolos	250 dias	Classificação por protocolo e uso do *payload* para tabela de RRs por quantidade de requisições com dados de longevidade.
(THOMAS; CLAYTON; BERESFORD, 2017)	8 Protocolos	1010 dias	Classificação por protocolo e uso do *payload* de modo restrito aos nomes de domínio mais utilizados em ataques.
(HEINRICH, 2017)	DNS	121 dias	Categorização de DNS e uso do *payload* para análise longitudinal sem avaliação de evolução.
(HEINRICH, 2019)	7 Protocolos	255 dias	Classificação e análise temporal por protocolo e uso do *payload* para análise por protocolo.
(HEINRICH; OBELHEIRO; MAZIERO, 2021)	9 Protocolos	731 dias	Classificação por protocolo e uso do *payload* para análise específica a nível de protocolo.
(KOPP; DIETZEL; HOHLFELD, 2021)	12 Protocolos	210 dias	Identificação por protocolo e sem uso de *payloads*.
(HEINRICH et al., 2022)	9 Protocolos	1312 dias	Classificação geográfica de vítimas por IP e sem uso de *payloads*.
Este trabalho	9 Protocolos	1278 dias	Classificação por protocolo e uso de *payload* para análise longitudinal de série temporal.

Fonte: Autor (2023)

3.2 DEFINIÇÃO DO PROBLEMA

Ataques distribuídos de negação de serviço estão cada vez mais frequentes e fáceis de serem realizados, como demonstra o aumento de ataques DDoS ao longo dos anos. Ataques DDoS por reflexão, ou DRDoS, têm se mostrado difíceis de mitigar, uma vez que o tráfego que atinge as vítimas provém de um número potencialmente elevado de refletores que atuam apenas como intermediários, sem vinculação com os reais responsáveis pelos ataques. A amplificação obtida em ataques DRDoS depende diretamente dos *payloads* das requisições enviadas para os refletores. Ao modificar o *payload* de uma requisição, é possível obter respostas diferentes, com mais ou menos bytes. Dessa forma, os *payloads* usados em ataques DRDoS podem evoluir com vistas a maximizar a amplificação produzida. Outra possível causa para a evolução dos *payloads* de ataque é a adoção de medidas de mitigação, como a depreciação do QTYPE `ANY` em consultas

DNS (ABLEY et al., 2019).

No entanto, embora existam diversos trabalhos que consideram *payloads* dos ataques para a caracterização, mapeamento geográfico e identificação de tráfego, as características e evolução ao longo do tempo dos *payloads* das requisições não são discutidas na literatura. Os estudos existentes consideram que os *payloads* de ataque permanecem largamente estáticos, possivelmente sendo os mesmos que eram empregados quando os ataques foram descobertos. Como discutido acima, essa premissa de que esses *payloads* ficam inalterados carece de verificação empírica.

3.3 PROPOSTA

A proposta consiste na análise de evolução de dados gerais e de *payloads* de nove protocolos (Chargen, DNS, NTP, Memcached, QOTD, SSDP, CoAP, CLDAP e Steam) implementados pelo *honeypot* MP-H. O trabalho analisa dados de ataques DRDoS e realiza uma observação longitudinal dos *payloads* utilizados pelos atacantes para observar diferenças e possíveis evoluções ao longo do período de coleta de 1278 dias.

O contexto de análise de evolução de dados gerais tem como foco a observação das quantidades de requisições, ataques e vítimas distintas para cada protocolo, além de observações sobre dados gerais que agrupam todos os protocolos. Já o contexto de análise da evolução de *payloads* é específico por protocolo, e busca analisar quais as mudanças ocorreram ao longo do tempo nos *payloads* usados nos ataques DRDoS.

3.4 CONSIDERAÇÕES DO CAPÍTULO

Neste capítulo, apresentam-se os trabalhos relacionados na literatura que analisam e/ou caracterizam ataques distribuídos de negação de serviço por reflexão. A seguir, foram definidos o problema e a proposta deste trabalho, que consiste na análise de evolução de dados de ataques DRDoS, considerando não apenas os volumes de tráfego mas também os *payloads* usados em ataques, que é uma lacuna identificada na literatura. O Capítulo 4 apresenta e discute os resultados desta dissertação.

4 COLETA E ANÁLISE DE DADOS

Para caracterizar a evolução dos ataques DRDoS, foram analisados dados coletados por um *honeypot* MP-H entre 30/09/2018 e 31/03/2022. A Seção 4.1 descreve a coleta de dados. A Seção 4.2 apresenta definições adotadas na análise dos dados. A Seção 4.3 faz observações gerais sobre o tráfego coletado. A Seção 4.4 traça a evolução de ataques e requisições para cada protocolo. A Seção 4.5 analisa os *payloads* usados nos ataques. A Seção 4.6 faz uma discussão dos resultados obtidos.

4.1 COLETA DE DADOS

A implantação do MP-H ocorreu na rede da UDESC, e a coleta aconteceu 24 horas por dia, 7 dias por semana. O *honeypot* possui um IP fixo globalmente roteável e está exposto diretamente à Internet, isto é, não está atrás de um *firewall* nem sofre tradução de endereços (*network address translation*, NAT). 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);

O MP-H atualmente possui suporte para nove protocolos baseados em UDP (Chargen, DNS, NTP, Memcached, QOTD, SSDP, CoAP, CLDAP e Steam) sobre IPv4, e está operando desde setembro de 2018. CoAP e CLDAP foram incorporados em março e julho de 2020, respectivamente, ao passo que os demais estão presentes desde o início das operações. O *honeypot* é projetado para se comportar como um refletor: ele aceita requisições e retorna respostas que parecem genuínas, registrando o tráfego recebido. O MP-H limita o tráfego de resposta a cinco respostas por endereço IP de origem por dia, minimizando sua contribuição nos ataques DRDoS para os quais é usado. Mais detalhes sobre a arquitetura e o funcionamento do MP-H podem ser encontrados em (HEINRICH, 2019).

4.2 DEFINIÇÕES ADOTADAS

Todo o tráfego recebido por um *honeypot* pode ser considerado suspeito ou malicioso (HOEPERS; STEDING-JESSEN; CHAVES, 2007), uma vez que ele não hospeda nenhum serviço anunciado publicamente. No caso de um *honeypot* que imita um refletor, como o MP-H, o tráfego pode ser subdividido em duas classes básicas (HEINRICH, 2019):

1. Varreduras (*scans*), que buscam por hospedeiros e serviços disponíveis na rede;
2. Ataques DRDoS onde o MP-H é usado como refletor.

É possível considerar uma classe adicional de tráfego espúrio, que inclui casos em que o *honeypot* é erroneamente configurado como um servidor legítimo (por exemplo, um servidor DNS recursivo para um ou mais clientes).

Em um ataque DRDoS, cada refletor possui apenas visão parcial do ataque: ele observa apenas a sua contribuição para o ataque, não tendo conhecimento de quantos nem quais são os demais refletores envolvidos. Da mesma forma, o refletor não consegue determinar de forma precisa o início e o fim de um ataque. Portanto, para caracterizar ataques, é necessário adotar uma definição que permita classificar conjuntos de pacotes recebidos pelo *honeypot* como ataques. Este trabalho segue a mesma definição de ataque usada em trabalhos anteriores que utilizaram o MP-H (HEINRICH; OBELHEIRO; MAZIERO, 2021; HEINRICH et al., 2022):

> *Um ataque DRDoS consiste em um conjunto com no mínimo 5 requisições com mesmo endereço IP de origem e com espaçamento máximo de 60 segundos entre requisições consecutivas.*

Como as requisições em um ataque DRDoS usam IP *spoofing* (Seção 2.2), os endereços IP de origem dessas requisições correspondem a vítimas de ataques.

Para considerar a evolução temporal do tráfego DRDoS, os dados foram agrupados em trimestres, de acordo com os meses do ano: o primeiro trimestre vai de 01/01 a 31/03, o segundo de 01/04 a 30/06, e assim sucessivamente. Outros períodos de agregação foram avaliados e descartados: períodos maiores (ano, semestre) mostraram granularidade muito grossa para análise, ocultando variações relevantes, ao passo que períodos menores (bimestre, mês) tiveram característica oposta, indicando variações sem relevância. Os trimestres são representados como *ano/trimestre*; por exemplo, o terceiro trimestre de 2020 é representado como 2020/3.

4.3 OBSERVAÇÕES GERAIS

Os dados foram coletados entre 30/09/2018 e 31/03/2022, um período de 1.278 dias (3,6 anos). A Tabela 4 apresenta as estatísticas do tráfego coletado (gerais e por protocolo). O *honeypot* recebeu 46,5 bilhões (B) de requisições, correspondentes a 7,6 milhões (M) de ataques.

Tabela 4 – Requisições e ataques observados pelo *honeypot*.

Observações gerais	**Requisições**		**Ataques**	
	46.465.992.065	100,0%	7.554.509	100,0%
Observações por protocolo				
	Requisições		**Ataques**	
Chargen	15.016.833.587	32,3%	485.789	6,4%
CLDAP	23.769.021.425	51,2%	5.520.708	73,1%
CoAP	2.017.192	<0,1%	4.205	0,1%
DNS	314.331.639	0,7%	861.491	11,4%
Memcached	5.517.264.042	11,9%	290.886	3,9%
NTP	1.111.834.689	2,4%	131.948	1,7%
QOTD	573.224.446	1,2%	59.305	0,8%
SSDP	159.954.964	0,3%	199.880	2,6%
Steam	1.510.081	<0,1%	297	<0,1%

Fonte: Autor (2023)

Os ataques afetaram 1,4 M vítimas distintas, que foram associadas a 226 códigos de países usando a base de dados GeoLite2 (GEOLITE2, 2023).

A Tabela 5 apresenta a evolução anual de requisições, ataques e novas vítimas (endereços IP observados pelo *honeypot* pela primeira vez); os dados de 2018 e 2022 refletem anos incompletos (início da coleta em set/2018 e final em mar/2022). Dois aspectos merecem destaque. O primeiro diz respeito às novas vítimas: embora um número elevado fosse esperado para 2018 e 2019 (e mesmo 2020, pela adição de CoAP e CLDAP ao *honeypot*), observa-se que elas aparecem em grande número em todos os anos. Isso mostra que existe uma renovação de vítimas, e que o refletor não é usado apenas para atacar repetidamente os mesmos alvos. O segundo aspecto é o crescimento dos ataques em 2021, que foi mais de 3,2× o volume de ataques em 2019 e 2020.

Tabela 5 – Observações por ano. Os anos marcados com * são incompletos.

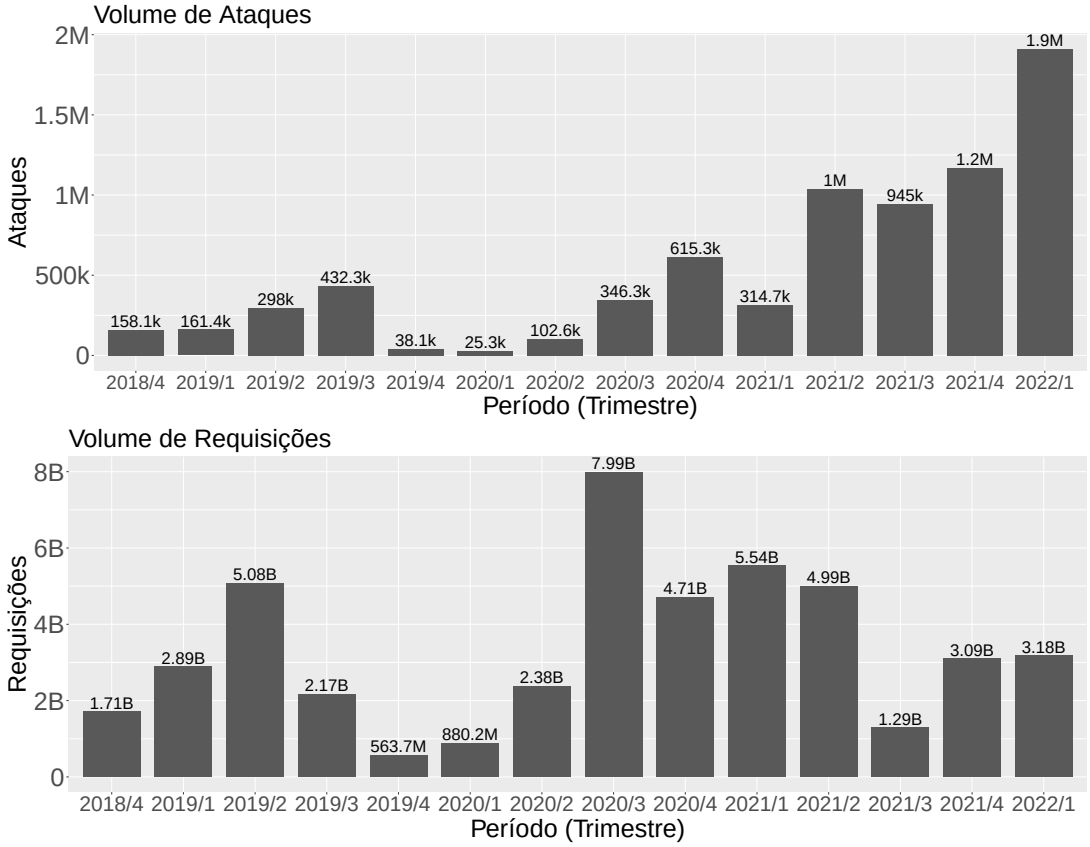
Ano	**Requisições**	**Ataques**	**Novas Vítimas**
2018*	1,70 B	158 k	50 k
2019	10,70 B	930 k	4479 k
2020	15,96 B	1,08 M	488 k
2021	14,91 B	3,47 M	355 k
2022*	3,17 B	1,91 M	34 k

Fonte: Autor (2023)

A Figura 4 mostra a quantidade de ataques e requisições para cada trimestre. Foram registrados em média 540 k ataques e 3,3 B requisições por trimestre. Em 2020/3 foi observado o maior volume de requisições (8,0 B), com 346 k ataques. O trimestre com mais ataques foi 2022/1, com 1,9 M ataques e 3,2 B requisições. O número de ataques teve um crescimento gradativo entre 2018/4 e 2019/3, com queda em 2019/4 e 2020/1, e retorno do crescimento (à

exceção de 2021/3), impulsionado pela adição de CLDAP ao MP-H. A quantidade de requisições apresentou um comportamento parecido entre 2018/4 e 2020/2, atingindo o pico em 2020/3 e passando a cair a partir de 2021/1. Quatro trimestres (2020/3 a 2021/2) concentram 50,2% das requisições e 32,9% dos ataques, ao passo que os três trimestres subsequentes (2021/3 a 2022/1) respondem por 16,4% das requisições e concentram 55,0% dos ataques. A correlação entre ataques e requisições por trimestre é fraca ($r = 0{,}07$). A comparação entre ataques e requisições mostra que os ataques foram em média mais intensos em 2019/2 e 2020/3, e que a intensidade média vem caindo desde 2021/2.

Figura 4 – Ataques e requisições por trimestre. Observar escalas diferentes no eixo *y*.

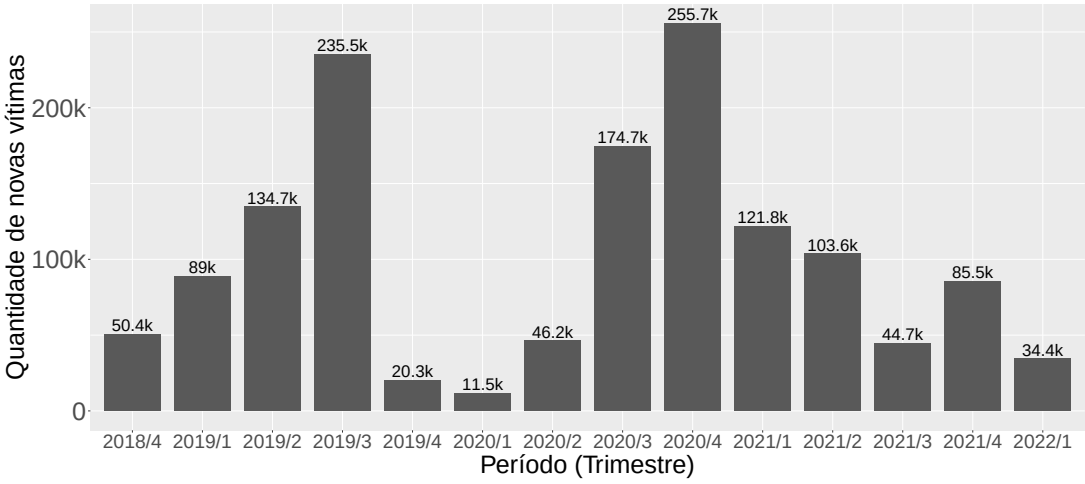


Fonte: Autor (2023)

A Figura 5 mostra a quantidade de novas vítimas observadas pelo *honeypot* a cada trimestre. Os primeiros trimestres (entre 2018/4 e 2019/3) tiveram um crescimento no número de novas vítimas. Isso é natural, advindo da descoberta e recrutamento do *honeypot* como refletor em ataques DRDoS. O aumento significativo em 2020/3 e 2020/4 pode ser atribuído à implantação do CLDAP no MP-H, que inicia um novo período de descoberta e recrutamento do refletor. É possível destacar que todos os trimestres apresentam milhares de novas vítimas, o que corrobora a renovação de vítimas apontada na discussão da Tabela 5. A quantidade de novas vítimas por trimestre tem correlação moderada ($r = 0{,}59$) com o número de requisições, e correlação fraca ($r = -0{,}03$) com o número de ataques (Figura 4).

A Figura 6 demonstra o volume de novas vítimas ao lado do volume de vítimas distintas

Figura 5 – Novas vítimas por trimestre.

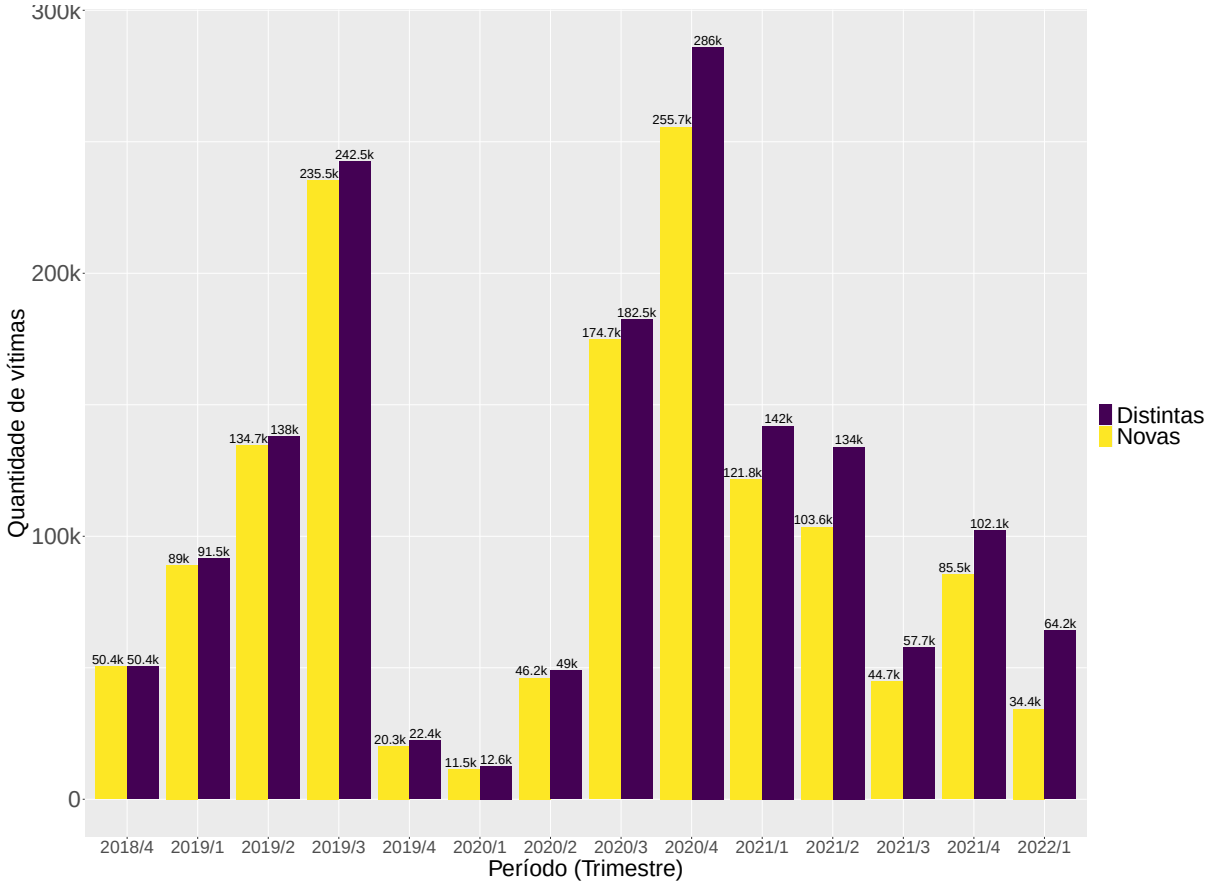


Fonte: Autor (2023)

por trimestre. Todos os trimestres apresentam uma porcentagem de novas vítimas em relação às vítimas distintas maior que 77,3%, exceto o último trimestre (2022/1), com 53,6%. Até o terceiro trimestre de 2020, mais de 90,8% das vítimas distintas dos trimestre eram de novas vítimas.

Ao analisar os dados de observação geral, é possível definir que existe uma tendência recente de crescimento no número de ataques, com redução da média de requisições por ataque. Além disso, os dados referentes as novas vítimas demonstram uma continuada renovação das vítimas de ataques, não somente em valores relativos à quantidade de vítimas distintas, mas também em valores absolutos.

Figura 6 – Vítimas novas e distintas por trimestre.



Fonte: Autor (2023)

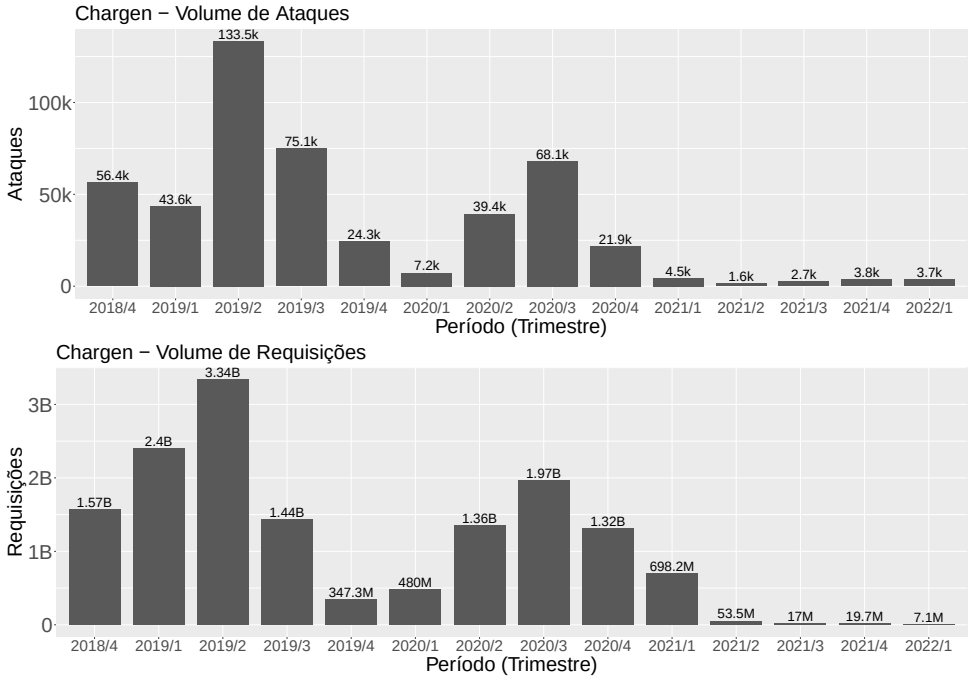
4.4 OBSERVAÇÕES POR PROTOCOLO

As observações por protocolo na Tabela 4 mostram que os dois protocolos com mais requisições (CLDAP e Chargen) e ataques (CLDAP e DNS) concentram 83,5% e 84,5% dos respectivos totais. O CLDAP aparece em primeiro tanto em requisições (51,2%) quanto em ataques (73,1%), o que é especialmente notável por ter sido o último protocolo incorporado ao MP-H, em julho de 2020. Embora a correlação entre requisições e ataques por protocolo seja forte ($r = 0{,}84$), há discrepâncias relevantes: DNS é o segundo protocolo com mais ataques (11,4% do total) mas apenas o sexto em volume de requisições (0,7% do total), enquanto Memcached responde por 11,9% das requisições e 3,9% dos ataques. As diferenças entre requisições e ataques refletem diferentes intensidades de ataque para os vários protocolos, com a média de requisições por ataque indo de 364,9 para o DNS a 30.912,3 para o Chargen. Fatores que contribuem para essas diferenças de intensidade incluem a amplificação alcançada com cada protocolo (alguns protocolos exigirão mais requisições para atingir um dado volume de tráfego para a vítima) e a disponibilidade de refletores (havendo mais refletores disponíveis, cada refletor pode receber uma carga menor de requisições em um ataque).

As Figuras 7 a 12 mostram os ataques e requisições por protocolo. O Chargen (Figura 7)

foi o protocolo com mais requisições até 2020/2, com mais de 54% do total. O ápice foi observado em 2019/2, com 134 k ataques e 3,34 B requisições. Entre 2018/4 e 2020/4 as variações no número de ataques acompanharam as do número de requisições. O número de ataque e requisições vem apresentando uma tendência geral de queda desde 2020/3, que tornou-se mais acentuada a partir de 2021/3. Uma exceção foi 2021/1, que teve um volume pequeno de ataques (4,5 k) e elevado de requisições (698,3 M), uma média de 154,8 k requisições por ataque (mais de 2,3× a segunda maior intensidade média, de 66,2 k em 2020/1).

Figura 7 – Ataques e requisições do Chargen. Observar escalas diferentes no eixo *y*.

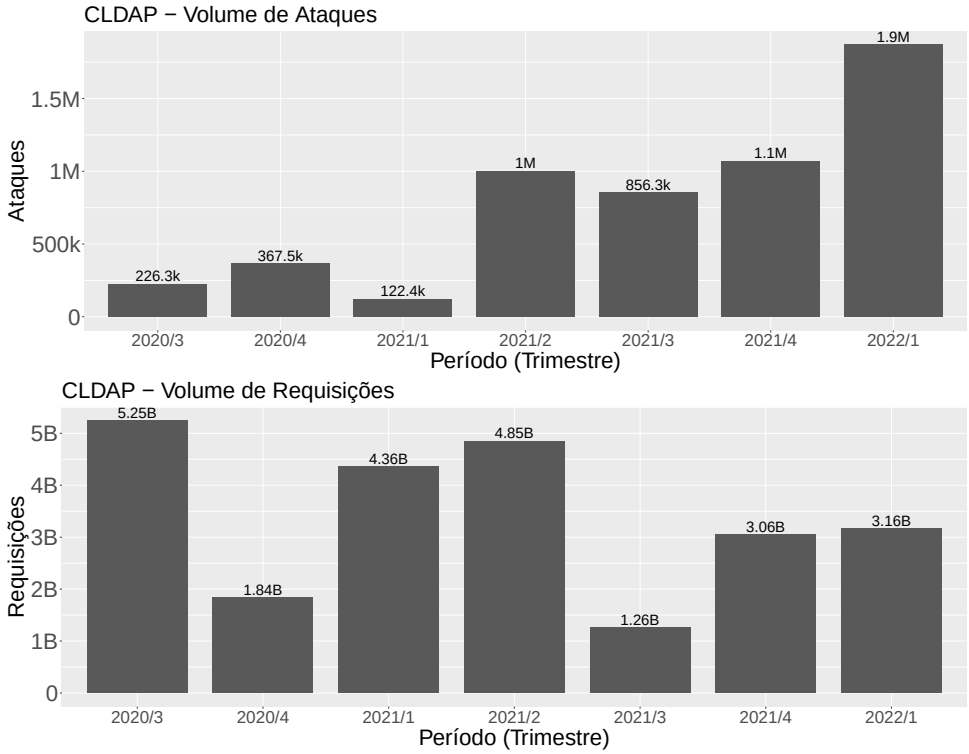


Fonte: Autor (2023)

A Figura 8 mostra a evolução do tráfego de CLDAP. Os dados iniciam em 2020/3 porque este protocolo só foi implantado no MP-H em julho de 2020. Observa-se um volume expressivo de requisições em todos os trimestres: cinco dos sete trimestres tiveram pelo menos 3,06 B requisições, e o mínimo foi de 1,26 B. Entre 2020/3 e 2021/2 teve-se um período de ataques mais intensos, com médias entre 4,8 k e 36,1 k requisições por ataque (em 2021/2 e 2021/1, respectivamente). A partir de 2021/3, tem-se uma tendência de aumento do número de ataques que não é acompanhada pelo número de requisições, o que representa ataques menos intensos (entre 1,4 k e 2,9 k requisições por ataque em média).

A Figura 9 apresenta o volume de ataques e requisições para o DNS. A única tendência identificável é uma queda no volume de ataques e requisições a partir de 2021/2. O período até 2020/3 (excetuando 2019/3) teve maior intensidade média de ataques, entre 869,2 e 5213,7 requisições por ataque; esse comportamento é semelhante ao observado para o CLDAP. A discrepância em 2019/3 deve-se a um período de 15 dias entre julho e agosto de 2019, que teve um crescimento de quase 10× no número diário de ataques; esse período teve uma predominância

Figura 8 – Ataques e requisições do CLDAP. Observar escalas diferentes no eixo *y*.



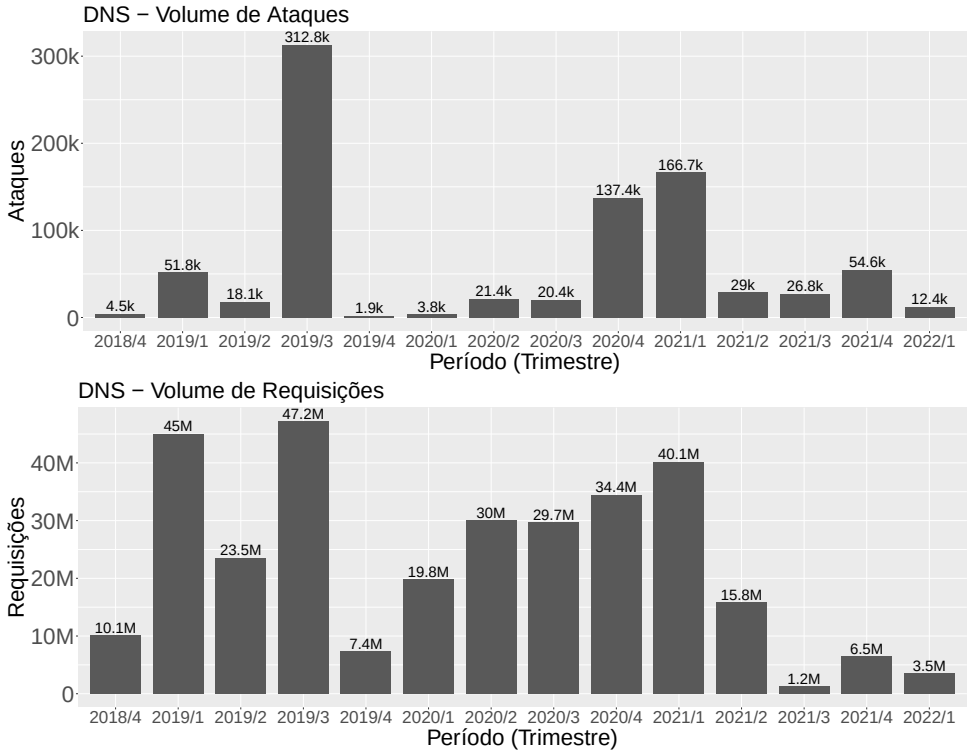
Fonte: Autor (2023)

de ataques de pouca intensidade (80% dos ataques tiveram até 127 requisições) que afetaram vítimas sem qualquer relação conhecida, e para os quais não foi possível encontrar explicação.

A Figura 10 mostra as quantidades de ataques e requisições do Memcached. Observa-se que o número de ataques tem uma tendência geral de queda desde o início (2018/4), que tornou-se acentuada a partir de 2021/1. A partir de 2019/3, as variações no número de ataques acompanharam as do número de requisições. Os maiores volumes de requisições foram observados em 2019/2 (1,62 B) e 2020/2 (978,5 M). Cabe destacar que os ataques com Memcached foram divulgados mais amplamente no fim de fevereiro de 2018 (MAJKOWSKI, 2018), mesmo mês em que o suporte a UDP passou a ser desabilitado por padrão no servidor (MEMCACHED, 2018). A mudança na configuração padrão tende a provocar a redução do número de refletores abertos: além dos servidores que foram explicitamente reconfigurados para desabilitar UDP, novos servidores foram instalados já sem a vulnerabilidade, o que também pode ter ocorrido com servidores existentes que tiveram o *software* atualizado. Assim, a evolução observada para o Memcached é compatível com o período entre a divulgação de uma vulnerabilidade de alto impacto e a sua remediação em larga escala, que representa uma janela de oportunidade que vai se fechando para os atacantes, que acabam migrando para outros vetores de ataque.

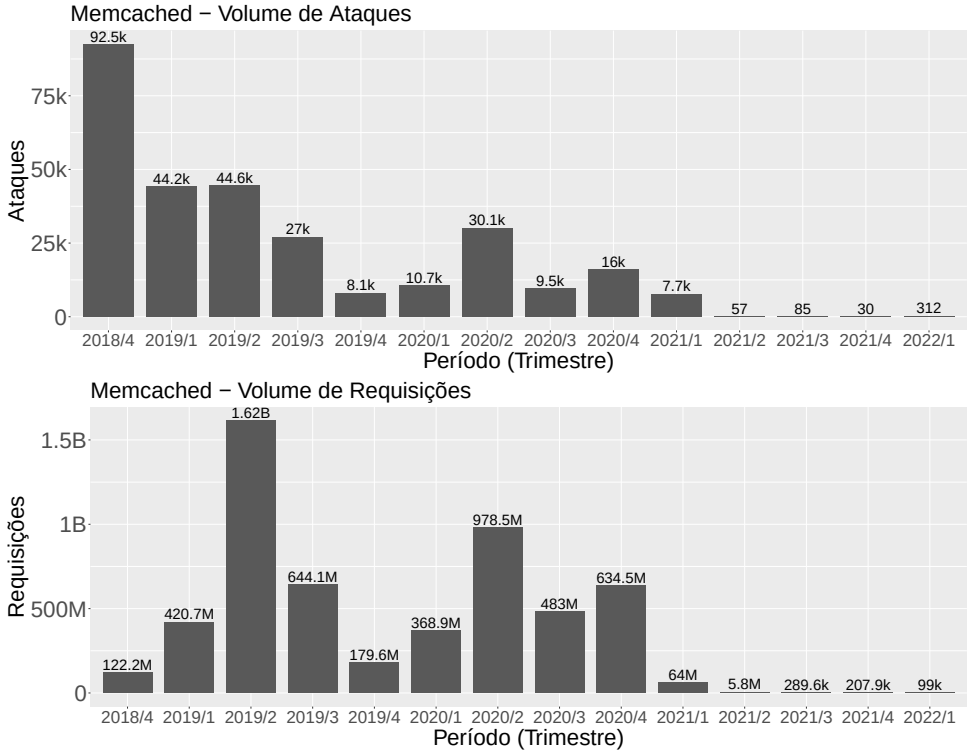
A Figura 11 apresenta o volume de ataques e requisições do protocolo QOTD. Os trimestres 2020/3 e 2020/4 concentraram os ataques (36,0 k, 60,7% do total) e requisições (373,7 M, 65,2% do total) referentes a esse protocolo. Antes de 2020/3, os ataques e requisições ficaram concentrados em 2019/2 e 2019/3, que juntos tiveram 90,4% dos ataques e 91,4% das requisições

Figura 9 – Ataques e requisições do DNS. Observar escalas diferentes no eixo *y*.



Fonte: Autor (2023)

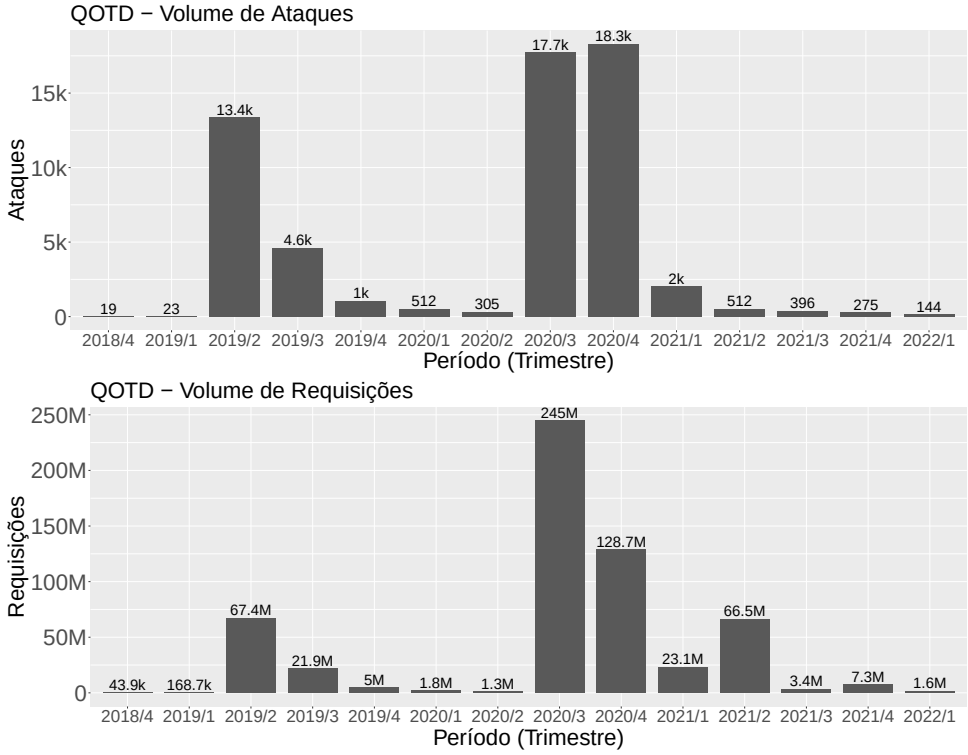
Figura 10 – Ataques e requisições do Memcached. Observar escalas diferentes no eixo *y*.



Fonte: Autor (2023)

do período. A partir de 2021/1, tanto ataques quanto requisições caíram significativamente, com exceção de 2021/2, que teve 66,5 M requisições.

Figura 11 – Ataques e requisições do QOTD. Observar escalas diferentes no eixo *y*.



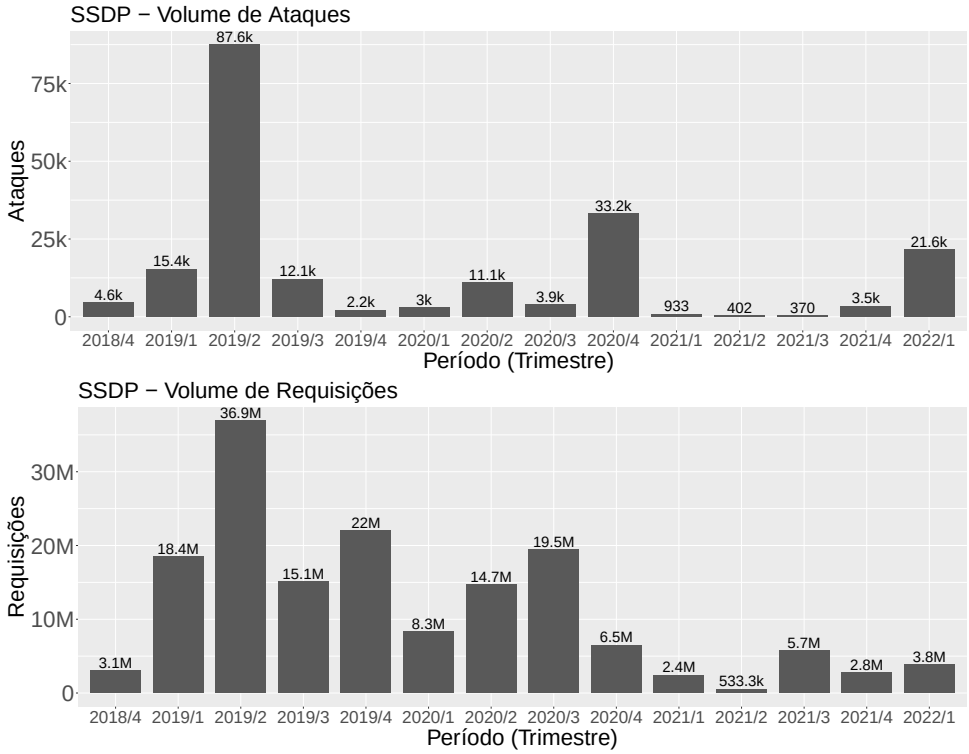
Fonte: Autor (2023)

A Figura 12 mostra os ataques e requisições do SSDP. O número de ataques é baixo no geral, superando 20 k em apenas três trimestres (2019/2, 2020/4 e 2022/1), e não exibe tendência. O período até 2020/4 concentrou as requisições SSDP, com 90,4% do total.

Os protocolos CoAP, NTP e Steam tiveram pouco destaque em termos de evolução. CoAP e Steam tiveram poucos ataques e requisições. Para CoAP, os ataques ficaram concentrados em 2021/4 (2817, 67,0% do total) e as requisições em 2020/4 (1,25 M, 61,8% do total). Para Steam, o destaque foi o trimestre 2020/3, que contabilizou 53 ataques e 1,5 M requisições (99,3% do total); houve mais ataques (155) em 2021/1, mas com um pequeno número de requisições (8952). Com relação ao NTP, houve forte concentração de ataques e requisições em alguns trimestres: ataques em 2020/4, 2021/3 e 2021/4 (112,0 k, 84,9% do total), e requisições em 2020/4 e 2021/1 (1,10 B, 98,9% do total).

A Figura 13 oferece uma visão mais abrangente, mostrando a evolução do *mix* de requisições recebidas por protocolo. Percebe-se que, em cada trimestre, poucos protocolos dominam o número de requisições, havendo uma variação dos protocolos envolvidos. Nos primeiros trimestres de coleta, Memcached e Chargen foram responsáveis por 90% do total de requisições. Em 2020/3 o MP-H incorporou o CLDAP, e o volume de requisições passou a ser dominado por este protocolo, que desde 2021/2 responde por mais de 97% do total. Embora o acréscimo de requisições de CLDAP tenha reduzido naturalmente a porcentagem de Memcached

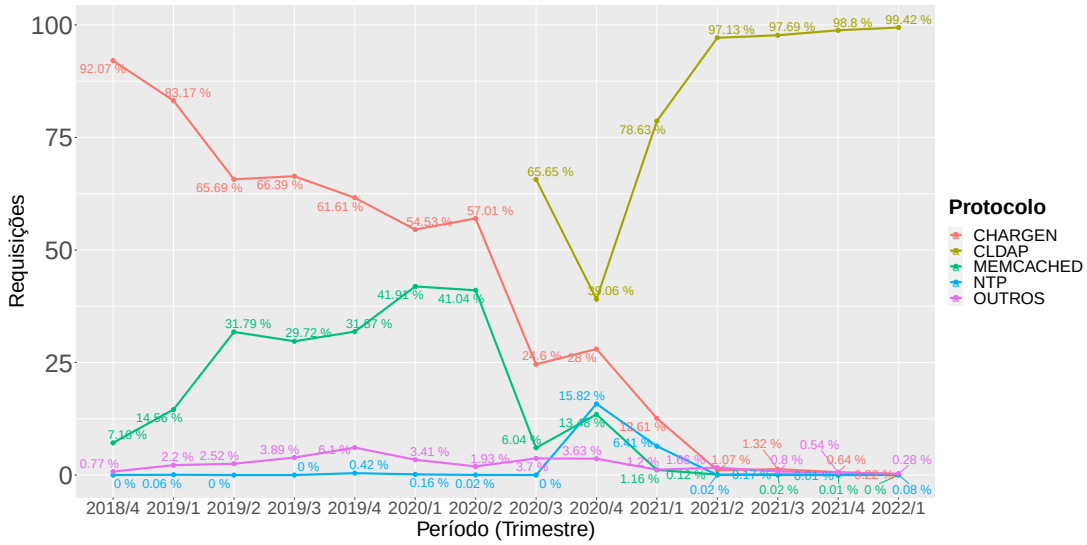
Figura 12 – Ataques e requisições do SSDP. Observar escalas diferentes no eixo *y*.



Fonte: Autor (2023)

e Chargen, estas vêm caindo também em valores absolutos desde 2020/2 (Chargen) e 2020/3 (Memcached), como mostram as Figuras 7 e 10.

Figura 13 – Evolução temporal das requisições por protocolo.



Fonte: Autor (2023)

4.5 ANÁLISE DE PAYLOADS

Os atacantes exploram os protocolos usados em ataques DRDoS de diferentes formas, visando simplificar a geração do tráfego de ataque e maximizar a amplificação obtida. A Tabela 6 resume como os protocolos suportados pelo MP-H são usados em ataques DRDoS, de acordo com a literatura (mais detalhes na Seção 2.2, página 21). Os protocolos estão classificados em três grupos, de acordo com o tipo de interação necessária para o atacante obter amplificação de tráfego. O grupo (A) contém protocolos cujas respostas independem do conteúdo das requisições recebidas. O grupo (B) contém protocolos com respostas que dependem das requisições, mas que, em ataques DRDoS, exibem uma forte preferência por um conjunto reduzido de requisições para maximizar a amplificação. Por fim, o grupo (C) agrega protocolos mais flexíveis, para os quais atacantes manipulam as requisições para obter maior amplificação. Para os grupos (A) e (B), o MP-H sintetiza respostas (seguindo a especificação de cada protocolo), e para o grupo (C) o *honeypot* faz *proxy* das requisições para um servidor real, repassando as respostas recebidas (HEINRICH; OBELHEIRO; MAZIERO, 2021). Em todos os casos, o MP-H limita o tráfego de resposta a cinco respostas por endereço IP de origem por dia, minimizando sua contribuição nos ataques DRDoS para os quais é usado.

Tabela 6 – Caracterização dos protocolos implementados pelo MP-H.

Grupo	**Protocolo**	**Interação/Resposta**
(A)	Chargen	Respostas de tamanho fixo, com 0 a 512 caracteres aleatórios, independente da requisição
	QOTD	Servidor envia uma citação aleatória com até 512 caracteres, independente da requisição
		(requisição típica)
(B)	CLDAP	Requisição `NETLOGON` que retorna uma lista de atributos suportados pelo servidor
	CoAP	Requisição `GET /.well-known/core` que retorna uma lista de funcionalidades suportadas pelo servidor
	NTP	Requisição `MONLIST` que retorna uma lista dos últimos 600 *hosts* que interagiram com o servidor
	SSDP	Requisições `M-SEARCH upnp:rootdevice` ou `ssdp:all` que retornam um conjunto de informações do serviço
	Steam	Particular a cada servidor e protocolo utilizado pelo jogo
(C)	DNS	Resposta depende do QNAME e QTYPE consultados
	Memcached	Duas possibilidades (1) consultar estatísticas padrões da aplicação, que geram uma resposta de tamanho fixo; ou (2) inserir as informações no banco de dados

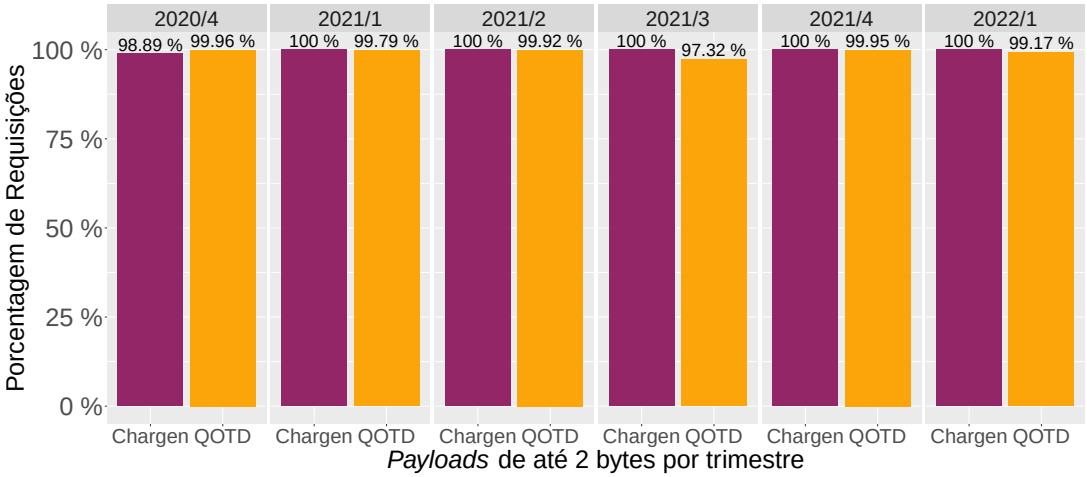
Fonte: Autor (2023)

Na sequência é feita a análise dos *payloads* das requisições processadas pelo *honeypot* e de sua evolução temporal. Como dados de *payloads* estão disponíveis a partir de 2020/4, a análise considera o período de 2020/4 até 2022/1. A avaliação dos protocolos segue o agrupamento apresentado na Tabela 6, discutindo as observações de acordo com o tipo de interação do

protocolo. Análises referentes ao número de requisições levam em consideração somente aquelas associadas a ataques (segundo a definição da Seção 4.2), e não as associadas a varreduras. O protocolo Steam teve pouco tráfego registrado, sem nenhum padrão discernível, e será excluído da análise.

Para os protocolos do grupo (A), Chargen e QOTD, os atacantes geralmente enviam requisições nulas (com *payload* vazio) ou com poucos bytes (HEINRICH; OBELHEIRO; MAZIERO, 2021), uma vez que as respostas independem da requisição. A Figura 14 apresenta a porcentagem de requisições com *payloads* de comprimento de até 2 bytes por trimestre para os protocolos do grupo (A). Nos trimestres avaliados, entre 98,9% e 100% das requisições Chargen tiveram *payloads* com 0 a 2 bytes de comprimento; os *payloads* não nulos continham majoritariamente os bytes `0` e/ou `1`. O QOTD apresenta um comportamento similar: nos trimestres avaliados, entre 97,3% e 99,96% das requisições tiveram *payloads* com 0 a 2 bytes de comprimento. Em 2022/1, houve uma incidência maior de mensagens com zero bytes. Os padrões mais comuns nas requisições não nulas foram os caracteres de quebra de linha (`\n` e `\r`). A análise mostra que, durante o período considerado, os protocolos do grupo (A) tiveram poucas mudanças nos *payloads*, que consistiram basicamente de mensagens muito pequenas (com até dois bytes).

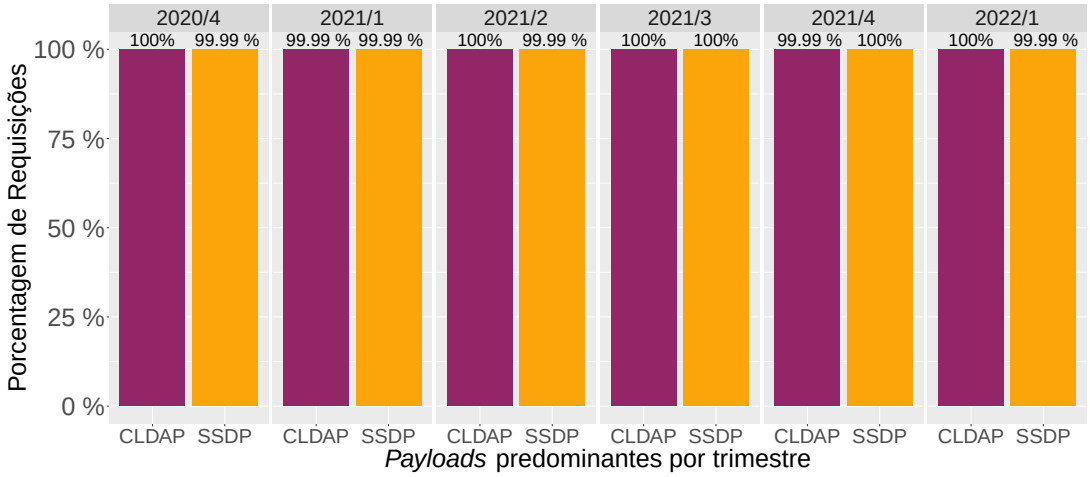
Figura 14 – Chargen e QOTD – porcentagem de requisições até 2 bytes.



Fonte: Autor (2023)

Para os protocolos do grupo (B), os ataques tendem a usar poucos tipos específicos de requisições, que são aquelas que produzem a maior amplificação para cada protocolo (HEINRICH; OBELHEIRO; MAZIERO, 2021). A Figura 15 apresenta a porcentagem de requisições que utilizam o *payload* predominante em ataques por trimestre. Dessa forma, para o CLDAP, entre 99,999995% e 100% dos *payloads* recebidos nos trimestres considerados foram requisições de `NETLOGON` que solicitam uma lista de atributos do servidor. No caso do SSDP, entre 99,999% e 100% das requisições foram comandos de busca (`M-SEARCH`) especificando como tipo de dispositivo uma das strings `upnp:rootdevice` ou `ssdp:all`. A mesma observação de utilização do `M-SEARCH` foi reportada por (HEINRICH, 2019) como predominante em 99,9% das requisições.

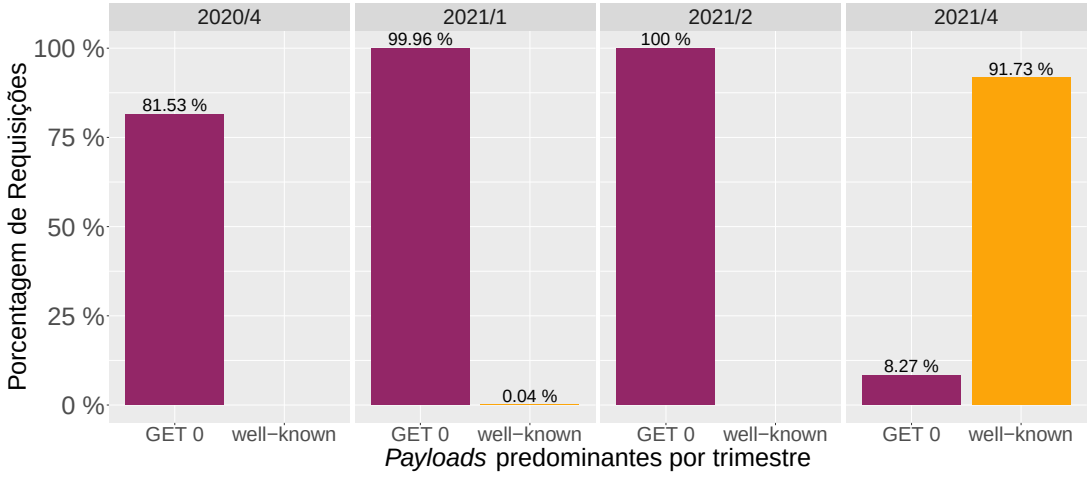
Figura 15 – CLDAP e SSDP – *payloads* predominantes por trimestre.



Fonte: Autor (2023)

No caso do CoAP, dos seis trimestres considerados, o *honeypot* não registrou ataques em 2021/3 e 2022/1. Embora a descrição original dos ataques (NETSCOUT, 2019) sugira que o tráfego DRDoS consiste em requisições `GET /.well-known/core`, esse tipo de mensagem é maioria apenas em 2021/4, com 91,7% das requisições. Nos demais trimestres predominaram mensagens consistindo em um `GET 0`, que representam de 81,5% a 100% das requisições, conforme demonstrado na Figura 16 que apresenta a porcentagem das requisições dos *payloads* predominantes por trimestre. Essas mensagens têm valores fixos para os campos *Message-ID* e *Token*, que deveriam ser únicos para cada requisição (SHELBY; HARTKE; BORMANN, 2014). Uma hipótese é que tais requisições sejam dirigidas a servidores Californium (ECLIPSE, 2022), uma implementação bastante disseminada de CoAP, que gera uma resposta de 500 bytes para essa requisição de 54 bytes (um fator de amplificação de 9,3×).

Figura 16 – CoAP – principais *payloads* por trimestre.

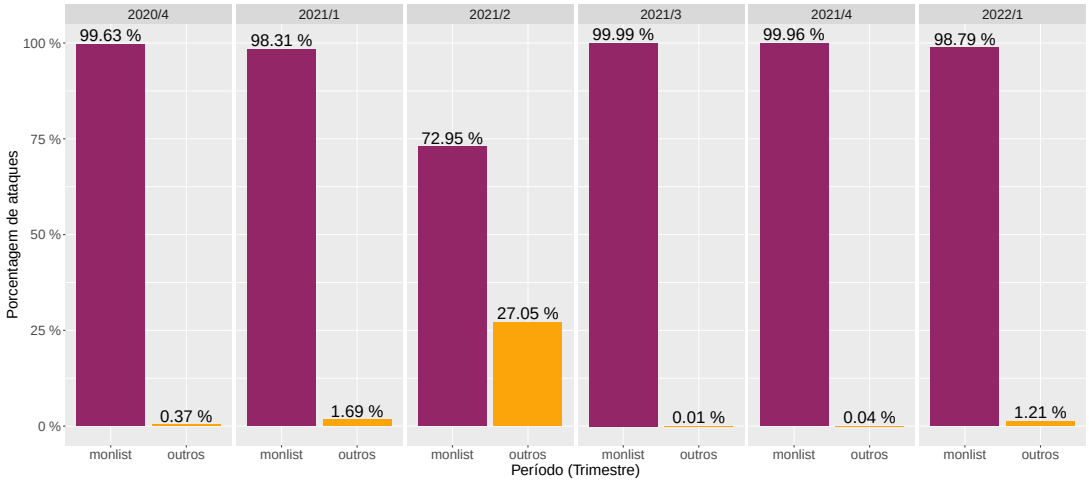


Fonte: Autor (2023)

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

DoS usando NTP (por exemplo, 99,9% em (HEINRICH; OBELHEIRO; MAZIERO, 2021)). A Figura 17 mostra a incidência de ataques com `MONLIST` em cada trimestre, em que durante o período considerado, houve mais de 99% de requisições `MONLIST` em todos os trimestres, com exceção de 2021/2, onde houve 27,05% de outras requisições. Parte desse tráfego diferente 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 17 – Incidência de `MONLIST` em ataques usando NTP.



Fonte: Autor (2023)

Os protocolos no grupo (C), DNS e Memcached, possuem uma maior variedade de *payloads*, por causa da sua flexibilidade. Como o tamanho das respostas depende intrinsecamente das requisições enviadas, atacantes tentam construir requisições pequenas que gerem respostas grandes, maximizando assim a amplificação de tráfego.

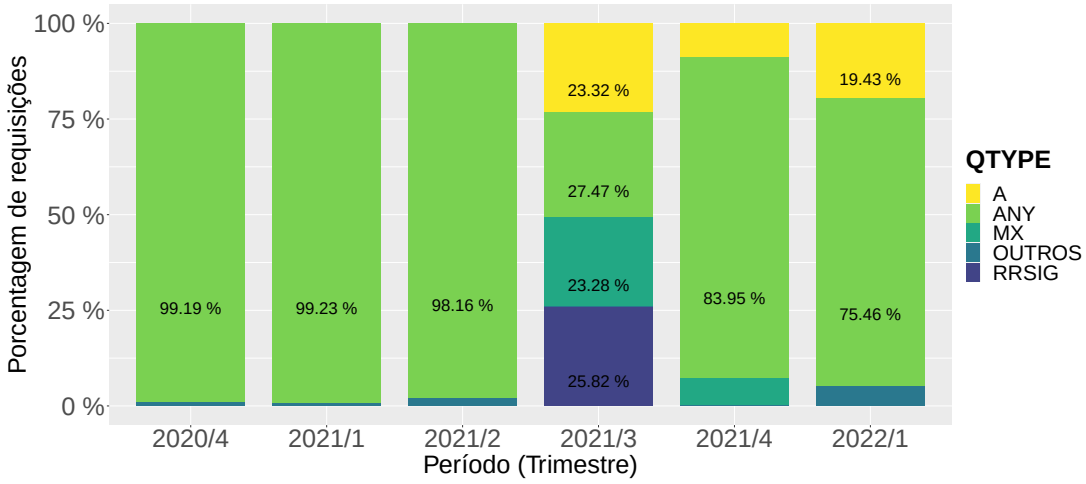
No DNS, o fator de amplificação depende do registro de recurso (*resource record*, RR) especificado na consulta. Um RR é formado por um nome de domínio (QNAME), um tipo (QTYPE) e uma classe (QCLASS), geralmente `IN` (Internet). Devido ao algoritmo de processamento de consultas do DNS (MOCKAPETRIS, 1987b), uma resposta pode conter vários RRs além do alvo da consulta, como uma lista de servidores DNS responsáveis pelo domínio do RR consultado e seus respectivos endereços IP. Uma análise dos RRs mais usados em ataques DRDoS não revelou nenhum padrão identificável de evolução, com variações de popularidade de trimestre para trimestre.

Ataques DRDoS frequentemente exploram as consultas com QTYPE `ANY`, que retornam um conjunto de RRs com o QNAME especificado na consulta e qualquer tipo (MOCKAPETRIS, 1987b). Estudos anteriores mostraram o predomínio desse tipo de requisição, com incidências de

93,7% em (HEINRICH, 2017), 99,8% em (HEINRICH, 2019) e cerca de 99% em (ANAGNOSTOPOULOS; LAGOS; KAMBOURAKIS, 2022). Essas consultas, cuja intenção era facilitar a depuração de problemas com o DNS, foram declaradas obsoletas em 2019 justamente em função do seu papel em ataques DRDoS (ABLEY et al., 2019); no entanto, muitos servidores ainda respondem a consultas `ANY`.

A Figura 18 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 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 (ABLEY et al., 2019), e a maioria das requisições de ataque ainda usam `ANY`.

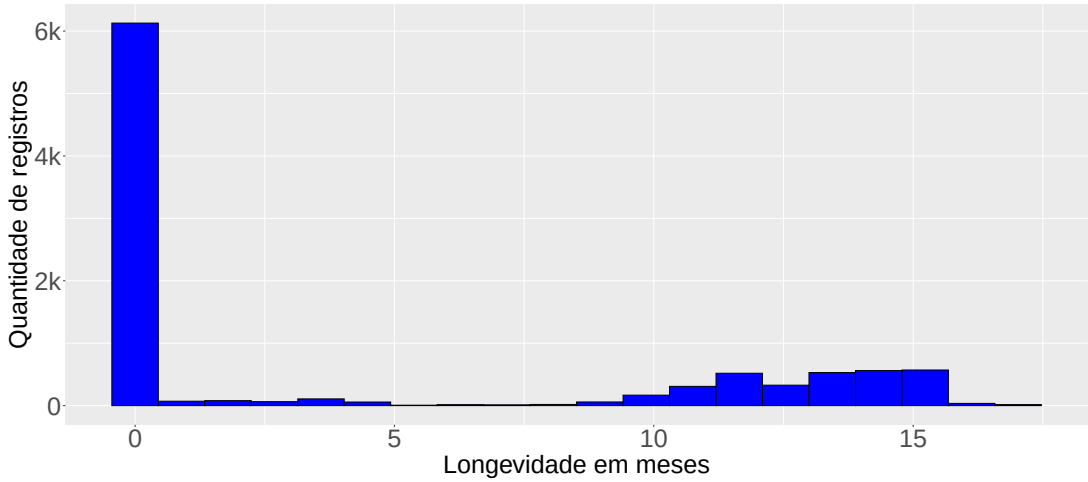
Figura 18 – Requisições DNS por QTYPE.



Fonte: Autor (2023)

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 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 o 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 19 mostra um histograma da longevidade dos RRs observados. Dos 9.663 RRs distintos, 6.048 (62,6%) têm baixa longevidade (um dia ou menos), 670 (6,9%) RRs têm longevidade entre um dia e 10 meses, e 2.945 (30,5%) possuem alta longevidade, superior a 10 meses. Entre os RRs com alta longevidade, 79,5% utilizam o QTYPE `A`.

Figura 19 – Longevidade de RRs em ataques DNS.



Fonte: Autor (2023)

A Tabela 7 apresenta os 10 RRs mais longevos. Esses RRs estiveram envolvidos em um número de ataques que vai de 22 a 69, e possuem fatores de amplificação pequenos, entre 1,24 e 1,81. Nove deles apresentam duas características peculiares: possuem QTYPE `MX` e QNAMEs sob o domínio de primeiro nível `.ae`, pertencente aos Emirados Árabes Unidos. É difícil explicar a persistência desses RRs, dada a pouca amplificação que eles oferecem.

Tabela 7 – Top 10 RRs com maior longevidade.

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

Fonte: Autor (2023)

Alguns RRs são mais utilizados em ataques do que outros, por fatores de amplificação ou facilidade de utilização de uma mesma ferramenta para ataques. A Tabela 8 compara alguns RRs que apareceram com destaque em trabalhos anteriores e que continuam sendo usados. O RR `1x1.cz ANY`, que foi o segundo RR com mais consultas em (HEINRICH, 2019) e o quinto em (HEINRICH, 2017), hoje aparece apenas na 3619ª posição (de 9663). Alguns RRs que tiveram destaque anteriormente (`. ANY` e `cpsc.gov`) aparecem com outros QTYPEs (`RRSIG`, `A`), igualmente com quedas significativas de popularidade.

Tabela 8 – RRs populares em estudos anteriores.

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
cpsc.gov	ANY	(HEINRICH, 2017)	A	10	3335

Fonte: Autor (2023)

O *Transaction ID* (TxID) é um identificador aleatório de 16 bits atribuído pelo cliente que realiza uma consulta DNS; ele é copiado pelo servidor na resposta, e pode ser usado pelo solicitante para casar respostas com as consultas pendentes (MOCKAPETRIS, 1987b). Como o identificador deve ser único para cada consulta (salvo retransmissões), o número de repetições esperadas de TxID para um conjunto de N consultas do mesmo cliente seria de $\frac{N}{2^{16}}$. A Tabela 9 mostra alguns desvios significativos do comportamento esperado para o TxID nas requisições observadas. O TxID 17767 foi utilizado em 77,4 k ataques, totalizando 9 M de requisições, entre 8 domínios diferentes. Esse número de repetições muito acima do esperado evidencia o uso de uma ferramenta automatizada de ataque, compartilhada entre ataques distintos.

Tabela 9 – Repetições de TxID em ataques DNS.

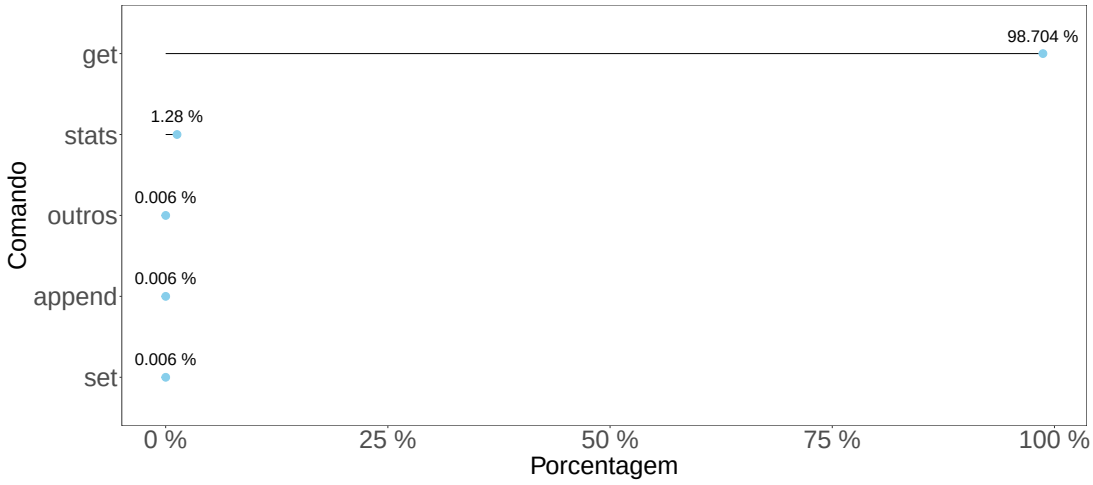
TxID	QNAME	Requisições	Repetição Observada	Repetição Esperada
17767	isc.org.	2,63 M	52.559	40
26566	peacecorps.gov.	9 M	34.570	137
17767	sl.	5,9 M	24.775	90
1	pizzaseo.com.	325 k	4.154	4
16049	irs.gov.	17 k	1.051	0,27

Fonte: Autor (2023)

As duas formas básicas de explorar Memcached para ataques DRDoS são (1) usando o comando `stats`, que obtém estatísticas do servidor, e (2) usando repetidamente o comando `get` para recuperar o conteúdo previamente associado a uma chave usando o comando `set` (MAJKOWSKI, 2018). A primeira forma é mais simples, mas oferece um menor potencial de amplificação do que a segunda. Em cinco dos seis trimestres observados, houve um predomínio absoluto da segunda forma: a porcentagem de requisições Memcached usando `stats` ficou entre 0,08% e 3,0%, enquanto que a porcentagem de requisições `get` variou entre 97,0% e 99,9%. A exceção foi o trimestre 2021/2, que teve 11,0% de requisições `stats` e 88,8% de `get`; mesmo com o aumento de 3,6× na proporção de `stats`, as requisições `get` ainda tiveram ampla maioria. Duas chaves ("`heian`" e "`s p h e`") foram usadas em 94,4% das requisições

`get`. Não foi possível discernir nenhum padrão nos valores associados a chaves (basicamente *strings* aleatórias), nem alguma evolução temporal de chaves ou valores. Ao computar os dados do Memcached de modo geral sem agrupar por trimestres, é possível observar na Figura 20 uma predominância do comando `get` em ataques realizados com esse protocolo. Essa mesma observação foi reportada em Heinrich (2019).

Figura 20 – Relação de ataques e comandos Memcached.



Fonte: Autor (2023)

A análise de *payloads* apresentada demonstrou poucas alterações na natureza das requisições utilizadas em ataques DRDoS. Contudo, uma tendência é apresentada em que há vestígios da adaptação de ataques DNS utilizando o QTYPE `ANY` para os do tipo `A` `MX`, possívelmente devido a queda de suporte a consultas do tipo `ANY`, que historicamente compunham quase a totalidade das requisições dos ataques desse protocolo.

4.6 DISCUSSÃO DOS RESULTADOS

A análise da evolução temporal dos dados coletados pelo *honeypot* revela características importantes dos ataques DRDoS envolvendo os protocolos considerados. Observando as quantidades de requisições e ataques recebidos, percebeu-se a partir de 2021/1 uma tendência de aumento do número de ataques e queda do volume médio de requisições por ataque. O aumento de ataques no período também foi reportado em (NETSCOUT, 2022).

Também foi possível observar uma migração de ataques de Chargen e Memcached para CLDAP; ainda que essa observação tenha sido influenciada pela implantação do CLDAP no MP-H em julho de 2020, é importante destacar que Chargen e Memcached caíram em números absolutos de ataques e requisições, não apenas em números relativos. Uma hipótese plausível é que essa migração esteja associada a uma redução na disponibilidade de refletores Chargen e Memcached. Esses protocolos podem ser filtrados em redes de provedores sem grandes consequências negativas, pois Chargen é um serviço legado, pouco usado para seu propósito original de resolução de problemas de rede, e Memcached pode ser usado com TCP, não apenas

UDP. De fato, o suporte a UDP no Memcached passou a ser desabilitado por padrão a partir da versão 1.5.6, de fevereiro de 2018 (MEMCACHED, 2018) à medida em que os servidores existentes passaram por atualizações de *software*, isso deve ter levado a uma queda no número de refletores Memcached, mesmo que os administradores responsáveis não tenham desabilitado UDP de forma deliberada. A redução no número de refletores Memcached é corroborada em (LAVRENOVS, 2021). Em contrapartida, embora haja a recomendação de desabilitar o uso de UDP em servidores *Active Directory*, uma pesquisa recente indica que o número de refletores CLDAP abertos vem se mantendo elevado, com mais de 12 mil refletores detectados (LUMEN, 2022).

Outra observação pertinente diz respeito à constante renovação de vítimas constatada no *honeypot*. Isso sugere que filtrar o tráfego com base nos pares de endereços IP de origem e destino envolvidos em ataques DRDoS possui eficácia limitada além de conter ataques em andamento, uma vez que não é comum que um refletor seja usado para atacar a mesma vítima de forma repetida.

A análise de *payloads* mostrou que, entre 2020/4 e 2022/1, houve pouca variação para os protocolos classificados nos grupos (A) e (B), que possuem requisições ou respostas fixas (Chargen, CLDAP, CoAP, NTP, QOTD e SSDP). A exceção foi o CoAP, onde houve uma mudança no tipo de requisição mais popular em 2021/4; o peso dessa conclusão deve ser relativizado tendo em vista o número relativamente pequeno de ataques usando CoAP observados pelo *honeypot*. Já para os protocolos do grupo (C), DNS e Memcached, que apresentam maior flexibilidade na geração de respostas, observou-se uma variação natural de *payloads* ao longo do período de análise. No caso do DNS, foram encontradas evidências de que o tráfego de ataque começou a se adaptar, nos dois últimos trimestres, para reduzir a incidência de consultas do tipo `ANY`, consideradas obsoletas desde 2019.

As principais defesas contra ataques DRDoS são *blackholing* (NAWROCKI et al., 2019) e o uso de serviços externos de proteção que realizam inspeção e filtragem de tráfego de ataque (*traffic scrubbing*) (MOURA et al., 2020). A pouca variação de *payloads* observada nos ataques DRDoS sugere que mecanismos que se baseiam na classificação de tráfego para descartar ou limitar a vazão podem constituir defesas eficazes dentro de redes de provedores (NUR, 2021; WICHTLHUBER et al., 2022).

Uma limitação do presente trabalho é que a análise se baseia em dados de um único *honeypot*. Assim, não é possível afirmar que as conclusões do estudo sejam representativas dos ataques DRDoS em geral, embora elas permaneçam válidas para esse refletor. Considerando a simplicidade do tráfego observado, porém, parece mais provável que outros refletores tenham diferenças em termos de seleção de vítimas e *mix*/volume de tráfego do que em termos de natureza das requisições.

4.7 CONSIDERAÇÕES DO CAPÍTULO

Esse capítulo apresentou uma análise dos dados coletados por 1278 dias utilizando o MP-H, um *honeypot* que imita o comportamento de um refletor. Foram observados e analisados dados de nove protocolos, com foco na evolução temporal do tráfego e dos *payloads*. A conclusão geral da análise é que, no período observado, houve poucas mudanças no modo de utilização dos refletores pelos atacantes. As exceções foram uma migração de Chargen e Memcached para outros protocolos (notadamente CLDAP) e a adaptação de ataques que utilizam o protocolo DNS como reação à queda de suporte a consultas do tipo `ANY`, que historicamente compunham quase a totalidade das requisições de ataque. A pouca mutabilidade das interações com os refletores favorece a elaboração de defesas baseadas nas características das requisições usadas nos ataques.

5 CONCLUSÃO

Ao longo da última década, ataques distribuídos de negação de serviço por reflexão (DRDoS) têm afetado a disponibilidade de serviços Internet. A utilização dos refletores propicia aos atacantes vantagens como amplificação de tráfego e maior anonimato. Fatores como a grande quantidade de refletores existentes, a descoberta continuada de novos vetores de reflexão, e o próprio crescimento da Internet, tanto em dispositivos conectados como em largura de banda disponível, possibilitam a realização de ataques cada vez maiores em volume de dados e quantidade de pacotes.

Observar ataques e entender como funcionam e evoluem é essencial para o desenvolvimento e aprimoramento de técnicas de mitigação. Analisando os estudos já realizados na literatura que contemplam ataques DRDoS, é possível observar uma lacuna na análise de evolução do tráfego enviado aos refletores.

Dessa forma, o objetivo dessa dissertação consistia na análise da evolução temporal do tráfego de ataques DRDoS, com foco nos *payloads* usados. Para atingir esse objetivo foi utilizado um *honeypot* MP-H, que imita um refletor, para analisar a evolução desses ataques entre o quarto trimestre de 2018 e o primeiro trimestre de 2022. Durante os 1.278 dias de coleta, o *honeypot* observou 7,6 M ataques contra 1,4 M vítimas, processando mais de 46 bilhões de requisições.

Ao realizar a análise dos resultados e comparação dos dados foi possível definir as principais constatações:

(i) Uma tendência recente de crescimento no número de ataques, com redução da média de requisições por ataque;

(ii) Uma migração do uso de Chargen e Memcached para CLDAP;

(iii) Uma continuada renovação das vítimas de ataques;

(iv) Adaptação de ataques DNS à queda de suporte a consultas do tipo `ANY`, que historicamente compunham quase a totalidade das requisições de ataque; e

(v) Poucas alterações na natureza das requisições usadas em ataques.

Embora os objetivos de análise de evolução de *payloads* tenham sido atingidos, algumas dificuldades foram encontradas na execução do projeto. Como a compreensão do funcionamento de protocolos legados ou que geralmente são abstraídos ao usuário final, e também uso de ferramentas para análise de dados e plotagem de gráficos como o R[1]. Essas dificuldades foram resolvidas com um trabalho de pesquisa na fundamentação dos conceitos e documentações dos protocolos e ferramenta.

Outro problema durante a execução do trabalho foi processar os *payloads* específicos de cada protocolo e transformar os dados de sequência de bytes para valores passíveis de serem

[1] <https://www.r-project.org/>

lidos e analisados por humanos. Essa questão foi solucionada observando especificações nas documentações e com a utilização de pacotes e bibliotecas de implementações disponíveis publicamente para realizar a transformação.

Para a continuação do trabalho dessa pesquisa, pretende-se ampliar o monitoramento de ataques DRDoS com mais *honeypots* de modo a disponibilizar o MP-H para ser implantado em novas redes. Outra forma de ampliar a observação de ataques é adicionar novos protocolos ao conjunto de protocolos suportados pelo MP-H como o SNMP, TFTP e DNSSEC, assim como adicionar o suporte a IPv6. Por fim, pode-se ainda mapear refletores abertos na Internet e correlacionar esses dados com os ataques observados pelos *honeypots* para realizar análises e possivelmente observar o mesmo ataque disperso por várias fontes.

REFERÊNCIAS

ABLEY, Joe et al. **Providing Minimal-Sized Responses to DNS Queries That Have QTYPE=ANY**. 2019. RFC 8482, Internet Engineering Task Force. Disponível em: <https://www.rfc-editor.org/rfc/rfc8482>. Citado 3 vezes nas páginas 26, 32 e 48.

AKAMAI. **Threat Advisory: RIPv1 Reflection DDoS**. [S.l.]: Akamai, 2016. Citado na página 24.

ANAGNOSTOPOULOS, Marios et al. DNS amplification attack revisited. **Computers & Security**, Elsevier, v. 39, p. 475–485, 2013. Citado 2 vezes nas páginas 29 e 31.

ANAGNOSTOPOULOS, Marios; LAGOS, Stavros; KAMBOURAKIS, Georgios. Large-scale empirical evaluation of DNS and SSDP amplification attacks. **Journal of Information Security and Applications**, Elsevier, v. 66, p. 103168, 2022. Citado na página 48.

ARENDS, Roy et al. **RFC 4033: DNS security introduction and requirements**. [S.l.]: RFC Editor, 2005. Citado na página 26.

ARENDS, Roy et al. **RFC 4035: Protocol modifications for the DNS security extensions**. [S.l.]: RFC Editor, 2005. Citado na página 26.

ARTEAGA, J; MEJIA, W. **CLDAP Reflection DDoS Threat Advisory**. [S.l.]: Apr, 2017. Citado 2 vezes nas páginas 24 e 25.

ASERT. **CoAP Attacks In The Wild | NETSCOUT**. 2019. <https://www.netscout.com/blog/asert/coap-attacks-wild>. (Accessed on 12/13/2022). Citado 2 vezes nas páginas 24 e 25.

BACKES, Michael et al. On the feasibility of TTL-based filtering for DRDoS mitigation. In: SPRINGER. **International Symposium on Research in Attacks, Intrusions, and Defenses**. [S.l.], 2016. p. 303–322. Citado na página 22.

BECKETT, David; SEZER, Sakir. HTTP/2 tsunami: Investigating HTTP/2 proxy amplification DDoS attacks. In: IEEE. **2017 Seventh International Conference on Emerging Security Technologies (EST)**. [S.l.], 2017. p. 128–133. Citado na página 24.

BHAGAT, Neeraj; ARORA, Bhavna. 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 26.

BIENKOWSKI, T. **No sooner did the ink dry: 1.7 tbps DDoS attack makes history**. [S.l.]: March, 2018. Citado na página 20.

BREWSTER, Thomas. **Cyber Attacks Strike Zimbabweans Around Controversial Election**. [S.l.]: August, 2013. Citado na página 20.

CERT. **1998 CERT Advisories**. 1998. <https://resources.sei.cmu.edu/asset_files/WhitePaper/1998_019_001_496180.pdf>. (Accessed on 12/12/2022). Citado na página 24.

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 14.

CERT/TCC. **1999 CERT Advisories**. 1999. <https://resources.sei.cmu.edu/asset_files/WhitePaper/1999_019_001_496184.pdf>. (Accessed on 01/03/2023). Citado na página 20.

CISA. **UDP-Based Amplification Attacks | CISA**. 2019. <https://www.cisa.gov/uscert/ncas/alerts/TA14-017A>. (Accessed on 12/12/2022). Citado na página 24.

CISA, Cybersecurity Infrastructure Security Agency. **UDP-Based Amplification Attacks | CISA**. 2019. <https://www.cisa.gov/uscert/ncas/alerts/TA14-017A>. (Accessed on 10/25/2022). Citado na página 24.

CONSORTIUM, SQLite. **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 33.

COX, Joseph. **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 20.

CZYZ, Jakub et al. Taming the 800 pound gorilla: The rise and decline of NTP DDoS attacks. In: **Proceedings of the 2014 Conference on Internet Measurement Conference**. [S.l.: s.n.], 2014. p. 435–448. Citado na página 24.

DAMAS, João; NEVES, Frederico A. C. **Preventing use of recursive nameservers in reflector attacks**. 2008. RFC 5358, Internet Engineering Task Force. Disponível em: <https://www.rfc-editor.org/rfc/rfc5358>. Citado na página 22.

DEAR, B. Perhaps the first denial-of-service attack. **PLATO History Blog**, 2010. Citado na página 20.

ECLIPSE. **Eclipse Californium™**. 2022. <https://www.eclipse.org/californium/>. (Accessed on 01/05/2023). Citado na página 46.

FERGUSON, Paul; SENIE, Daniel. **Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing**. 2000. RFC 2827 (BCP 38), Internet Engineering Task Force. Disponível em: <https://www.rfc-editor.org/rfc/rfc2827>. Citado na página 21.

FIELDING, Roy et al. **RFC2616: Hypertext Transfer Protocol–HTTP/1.1**. [S.l.]: RFC Editor, 1999. Citado na página 25.

GEOLITE2. **GeoLite2 Free Geolocation Data | MaxMind Developer Portal**. 2023. <https://dev.maxmind.com/geoip/geolite2-free-geolocation-data>. (Accessed on 01/05/2023). Citado na página 35.

GOLAND, Yaron Y. Simple service discovery protocol/1.0 operating without on arbiter. **IETF INTERNET-DRAFT draft-cai-ssdp-v1-03. txt**, 1999. Citado na página 26.

GONDIM, João JC; ALBUQUERQUE, Robson de Oliveira; OROZCO, Ana Lucila Sandoval. 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 na página 15.

GROUP, Technical Working et al. SNMP reflected amplification DDoS attack mitigation. **SNMP Reflected Amplification DDoS Attack Mitigation (August 1, 2012)**, 2012. Citado na página 24.

GUPTA, Brij B; BADVE, Omkar P. Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment. **Neural Computing and Applications**, Springer, v. 28, n. 12, p. 3655–3682, 2017. Citado na página 14.

HABERMAN, B. Control messages protocol for use with network time protocol version 4. **draft-ietf-ntp-mode-6-cmds-07, Internet Engineering Task Force, IETF Trust**, 2019. Citado na página 24.

HAQUE, Muhammad Reazul 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 20.

HEINRICH, Tiago. Análise longitudinal de dados do DNSpot. In: . [S.l.: s.n.], 2017. Citado 6 vezes nas páginas 29, 30, 31, 48, 49 e 50.

HEINRICH, Tiago. **Caracterização de ataques DRDoS usando honeypot**. Dissertação (Mestrado) — Universidade do Estado de Santa Catarina (UDESC), 2019. Disponível em: <https://www.udesc.br/arquivos/cct/id_cpmenu/1024/Disserta__o_completa_15699280495759_1024.pdf>. Citado 17 vezes nas páginas 15, 16, 17, 20, 21, 22, 24, 27, 30, 31, 33, 34, 45, 48, 49, 50 e 51.

HEINRICH, Tiago; LONGO, Felipe de Souza; OBELHEIRO, Rafael R. Experiências com um honeypot DNS: Caracterização e evoluão 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 2 vezes nas páginas 15 e 26.

HEINRICH, Tiago et al. How DRDoS attacks vary across the globe? In: **Proceedings of the 22nd ACM Internet Measurement Conference**. [S.l.: s.n.], 2022. p. 760–761. Citado 3 vezes nas páginas 30, 31 e 34.

HEINRICH, Tiago; OBELHEIRO, Rafael R. 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**. [S.l.: s.n.], 2019. p. 239–252. Citado na página 15.

HEINRICH, Tiago; OBELHEIRO, Rafael R; MAZIERO, Carlos 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 8 vezes nas páginas 15, 27, 30, 31, 34, 44, 45 e 47.

HOEPERS, Cristine; STEDING-JESSEN, Klaus; CHAVES, Marcelo H. P. C. 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 4 vezes nas páginas 15, 26, 27 e 34.

HOEPERS, Cristine et al. **Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos**. 2016. <https://www.cert.br/docs/whitepapers/dns-recursivo-aberto/>. (Accessed on 12/07/2022). Citado 2 vezes nas páginas 24 e 26.

HOFFMAN, P; SULLIVAN, A; FUJIWARA, K. **DNS Terminology**. 2019. RFC 8499, Internet Engineering Task Force. Disponível em: <https://www.rfc-editor.org/rfc/rfc8499>. Citado na página 25.

HUSÁK, Martin; VIZVÁRY, Martin. 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 na página 15.

JONKER, Mattijs 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 na página 14.

KARAMI, Mohammad; PARK, Youngsam; MCCOY, Damon. Stress testing the booters: Understanding and undermining the business of DDoS services. In: **Proceedings of the 25th International Conference on World Wide Web**. [S.l.: s.n.], 2016. p. 1033–1043. Citado na página 25.

KHANDELWAL, Swati. World's largest 1Tbps DDoS attack launched from 152,000 hacked smart devices. **The Hacker News**, 2016. Citado na página 20.

KHANTIMIROV, Ramil. **DDoS Attacks in 2022: Trends and Obstacles Amid Worldwide Political Crisis - Infosecurity Magazine**. 2022. <https://www.infosecurity-magazine.com/blogs/ddos-attacks-in-2022-trends/>. (Accessed on 01/02/2023). Citado na página 20.

KIM, Jungtae; KIM, Ik-Kyun; KANG, Koohong. Practical approaches to the DRDoS attack detection based on netflow analysis. 2016. Citado na página 26.

KINER, Emil; KONDURU, Satya. **How Google Cloud blocked largest Layer 7 DDoS attack yet, 46 million rps | Google Cloud Blog**. 2022. <https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps>. (Accessed on 01/08/2023). Citado na página 14.

KOPP, Daniel; DIETZEL, Christoph; HOHLFELD, Oliver. DDoS never dies? an IXP perspective on DDoS amplification attacks. In: SPRINGER. **International Conference on Passive and Active Network Measurement**. [S.l.], 2021. p. 284–301. Citado 2 vezes nas páginas 30 e 31.

KRÄMER, Lukas 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 15, 27, 29, 30 e 31.

KUMAR, Sanjeev. Smurf-based distributed denial of service (DDoS) attack amplification in internet. In: IEEE. **Second International Conference on Internet Monitoring and Protection (ICIMP 2007)**. [S.l.], 2007. p. 25–25. Citado na página 24.

LABS, NLnet. **NLnet Labs - Unbound - About**. 2019. <https://nlnetlabs.nl/projects/unbound/about/>. Citado na página 33.

LAVRENOVS, Arturs. Towards remediating DDoS attacks. In: **16th International Conference on Cyber Warfare and Security (ICCWS 2021)**. [S.l.: s.n.], 2021. Citado na página 52.

LEMOS, Robert. **History Shows DDoS Volumes to Keep Rising Despite Mitigation Efforts**. 2018. Disponível em: <https://www.eweek.com/security/how-ddos-attacks-techniques-have-evolved-over-past-20-years/>. Citado na página 20.

LOHRMANN, Dan. **Hacktivism and DDoS Attacks Rise Dramatically in 2022**. 2022. <https://www.govtech.com/blogs/lohrmann-on-cybersecurity/hacktivism-and-ddos-attacks-rise-dramatically-in-2022>. (Accessed on 01/02/2023). Citado na página 20.

LONG, Neil; THOMAS, Rob. Trends in denial of service attack technology. **CERT Coordination Center**, v. 648, p. 651, 2001. Citado na página 18.

LOPES, Rogério Wilson. **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 20.

LUMEN. **CLDAP Reflectors on the Rise Despite Best Practice**. 2022. Lumen blog. <https://tinyurl.com/56zxdtj7>. Citado na página 52.

MAJKOWSKI, Marek. **Stupidly Simple DDoS Protocol (SSDP) generates 100 Gbps DDoS**. 2017. <https://blog.cloudflare.com/ssdp-100gbps/>. (Accessed on 12/12/2022). Citado 2 vezes nas páginas 24 e 26.

MAJKOWSKI, Marek. **Memcrashed – Major Amplification Attacks from UDP Port 11211**. 2018. Cloudflare blog. <https://tinyurl.com/fpyw4ucc>. Citado 2 vezes nas páginas 40 e 50.

MEHRDAD, Sarmad et al. Cyber-physical resilience of electrical power systems against malicious attacks: A review. **Current Sustainable/Renewable Energy Reports**, Springer, v. 5, n. 1, p. 14–22, 2018. Citado na página 20.

MEMCACHED. **Github Release Notes 156 · memcached/memcached Wiki**. 2018. <https://github.com/memcached/memcached/wiki/ReleaseNotes156>. (Accessed on 01/05/2023). Citado 2 vezes nas páginas 40 e 52.

MEMCACHED. **Memcached - a distributed memory object caching system**. 2022. <https://memcached.org/>. (Accessed on 10/25/2022), <https://www.memcached.org/>. Citado 2 vezes nas páginas 23 e 33.

MENSCHER, Damian. **Identifying and protecting against the largest DDoS attacks | Google Cloud Blog**. 2020. <https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks>. (Accessed on 01/02/2023). Citado 2 vezes nas páginas 19 e 20.

MILLS, David L. et al. **Network Time Protocol Version 4: Protocol and Algorithms Specification**. 2010. RFC 5905, Internet Engineering Task Force. Disponível em: <https://www.rfc-editor.org/rfc/rfc5905>. Citado na página 24.

MIRKOVIC, Jelena; REIHER, Peter. 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 2 vezes nas páginas 14 e 21.

MOCKAPETRIS, Paul. **Domain Names – Concepts and Facilities**. 1987. RFC 1034, Internet Engineering Task Force. Disponível em: <https://www.rfc-editor.org/rfc/rfc1034>. Citado na página 25.

MOCKAPETRIS, Paul V. **Domain Names – Implementation and Specification**. 1987. RFC 1035, Internet Engineering Task Force. Disponível em: <https://www.rfc-editor.org/rfc/rfc1035>. Citado 4 vezes nas páginas 25, 26, 47 e 50.

MOORE, David et al. Inside the slammer worm. **IEEE Security & Privacy**, IEEE, v. 1, n. 4, p. 33–39, 2003. Citado na página 20.

MOURA, Giovane C. M. et al. Into the DDoS maelstrom: A longitudinal study of a scrubbing service. In: **5th International Workshop on Traffic Measurements for Cybersecurity (WTMC 2020)**. Genova, Italy: [s.n.], 2020. Citado 2 vezes nas páginas 22 e 52.

NAWROCKI, Marcin et al. Down the black hole: Dismantling operational practices of BGP blackholing at IXPs. In: **Proceedings of the Internet Measurement Conference**. [S.l.: s.n.], 2019. p. 435–448. Citado 2 vezes nas páginas 22 e 52.

NAZARIO, Jose. DDoS attack evolution. **Network Security**, Elsevier, v. 2008, n. 7, p. 7–10, 2008. Citado 2 vezes nas páginas 18 e 19.

NETSCOUT. **CoAP Attacks In The Wild**. 2019. ASERT blog. <https://tinyurl.com/3ctv2ewp>. Citado na página 46.

NETSCOUT. **Historical DDoS Attack Map, August 28, 2020 | NETSCOUT Omnis Threat Horizon**. 2020. <https://horizon.netscout.com/?filters=destination.country.NZ&mapPosition=18.13~50.43~1.00&time=20200828-055034>. (Accessed on 01/02/2023). Citado na página 20.

NETSCOUT. **NETSCOUT THREAT INTELLIGENCE REPORT - The Long Tail of Attacker Innovation**. 2021. <https://www.netscout.com/sites/default/files/2021-09/ThreatReport_1H2021_FINAL.pdf>. (Accessed on 01/02/2023). Citado na página 20.

NETSCOUT. **DDoS Threat Intelligence Report – Findings from 1st Half 2022**. 2022. <https://tinyurl.com/3w9ws2tx>. Citado na página 51.

NEWMAN, Lily Hay. Github survived the biggest DDoS attack ever recorded. **Wired**, v. 1, 2018. Citado 3 vezes nas páginas 20, 23 e 24.

NIST. **NVD - CVE-1999-1379**. 1999. <https://nvd.nist.gov/vuln/detail/CVE-1999-1379>. (Accessed on 01/09/2022). Citado na página 20.

NOLLA, Alejandro. **Amplification DDoS attacks with game servers**. Grenoble, France: [s.n.], 2013. 73–83 p. <https://tinyurl.com/4kkzrs64>. Citado na página 24.

NUR, Abdullah Yasin. Combating DDoS attacks with fair rate throttling. In: IEEE. **2021 IEEE International Systems Conference (SysCon)**. [S.l.], 2021. p. 1–8. Citado na página 52.

PAXSON, Vern. 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 3 vezes nas páginas 15, 21 e 22.

POSTEL, Jon. **Character Generator Protocol**. 1983. RFC 864, Internet Engineering Task Force. Disponível em: <https://www.rfc-editor.org/rfc/rfc864>. Citado na página 24.

POSTEL, Jon. **Quote of the Day Protocol**. 1983. RFC 865, Internet Engineering Task Force. Disponível em: <https://www.rfc-editor.org/rfc/rfc865>. Citado na página 24.

PRINCE, M. **The DDoS That Almost Broke the Internet**. March, 2013. Disponível em: <https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet>. Citado na página 20.

PROLEXIC. **An Analysis of DRDoS SNMP/NTP/CHARGEN Reflection Attacks - Part II of the DRDoS White Paper Series- Prolexic Technical White Paper**. 2013. <https://silo.tips/download/an-analysis-of-drdos-snmp-ntp-chargen-reflection-attacks>. (Accessed on 12/12/2022). Citado na página 24.

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 20.

PROVOS, Niels; HOLZ, Thorsten. **Virtual honeypots: from botnet tracking to intrusion detection**. [S.l.]: Pearson Education, 2007. Citado na página 27.

RANGAPUR, Aman; KANAKAM, Tarun; JUBILSON, Ajith. DDoSDet: An approach to detect DDoS attacks using neural networks. **arXiv preprint arXiv:2201.09514**, 2022. Citado na página 14.

RIJSWIJK-DEIJ, Roland van; SPEROTTO, Anna; PRAS, Aiko. DNSSEC and its potential for DDoS attacks: a comprehensive measurement study. In: **Proceedings of the 2014 Conference on Internet Measurement Conference**. [S.l.: s.n.], 2014. p. 449–460. Citado 2 vezes nas páginas 24 e 26.

ROSSOW, Christian. Amplification hell: Revisiting network protocols for DDoS abuse. In: **NDSS**. [S.l.: s.n.], 2014. Citado 9 vezes nas páginas 14, 15, 21, 22, 23, 24, 26, 29 e 31.

RYBA, Fabrice J et al. Amplification and DRDoS attack defense–a survey and new perspectives. **arXiv preprint arXiv:1505.07892**, 2015. Citado na página 20.

SHELBY, Zach; HARTKE, Klaus; BORMANN, Carsten. **The Constrained Application Protocol (CoAP)**. 2014. RFC 7252, Internet Engineering Task Force. Disponível em: <https://www.rfc-editor.org/rfc/rfc7252>. Citado 2 vezes nas páginas 25 e 46.

SHIELD, AWS. Threat landscape report-q1 2020. **Amazon, Seattle, WA, USA**, 2020. Citado na página 20.

SHIREY, Robert. **Internet Security Glossary, version 2**. 2007. RFC 4949, Internet Engineering Task Force. Disponível em: <https://www.rfc-editor.org/rfc/rfc4949>. Citado na página 18.

SIEKLIK, Boris; MACFARLANE, Richard; BUCHANAN, William J. Evaluation of TFTP DDoS amplification attack. **computers & security**, Elsevier, v. 57, p. 67–92, 2016. Citado na página 24.

SPITZNER, Lance. Honeypots: Catching the insider threat. In: **Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC)**. [S.l.: s.n.], 2003. Citado na página 27.

SUBRAMANI, Karthika; PERDISCI, Roberto; KONTE, Maria. 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 24.

THOMAS, Daniel R; CLAYTON, Richard; BERESFORD, Alastair 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 5 vezes nas páginas 14, 15, 16, 29 e 31.

TOH, Alethea. **Azure DDoS Protection—2021 Q3 and Q4 DDoS attack trends | Azure Blog and Updates | Microsoft Azure**. 2022. <https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021-q3-and-q4-ddos-attack-trends/>. (Accessed on 01/08/2023). Citado na página 14.

UTECH, Guilherme R; OBELHEIRO, Rafael 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 24.

VALVE. **Steam powered**. 2023. <https://store.steampowered.com/>. (Accessed on 01/03/2023). Citado na página 26.

WELZEL, Arne; ROSSOW, Christian; BOS, Herbert. 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 14.

WICHTLHUBER, Matthias et al. IXP Scrubber: Learning from blackholing traffic for ML-driven DDoS detection at scale. In: **Proceedings of the ACM SIGCOMM 2022 Conference**. [S.l.: s.n.], 2022. p. 707–722. Citado na página 52.

WOODY, Carol; MEAD, Nancy; SHOEMAKER, Dan. Foundations for software assurance. In: IEEE. **2012 45th Hawaii International Conference on System Sciences**. [S.l.], 2012. p. 5368–5374. Citado na página 20.

YOUNG, Alan. **Connection-less Lightweight X.500 Directory Access Protocol**. [S.l.], 1995. Disponível em: <https://www.rfc-editor.org/rfc/rfc1798>. Citado na página 25.

ZETTER, Kim. Lazy hacker and little worm set off cyberwar frenzy. **Wired News. http://www.wired.com/threatlevel/2009/07/mydoom**, 2009. Citado na página 20.