Caracterização de *Payloads* Usados em Ataques Distribuídos de Negação de Serviço por Reflexão (DRDoS)

Rafael Tenfen[1]

[1] Universidade do Estado de Santa Catarina (UDESC)
Departamento de Ciência da Computação
Mestrado em Computação Aplicada

rafaeltenfen.rt@gmail.com

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

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

1. Introdução

A negação de serviço, ou DoS *(Denial of Service)*, consiste em provocar a indisponibilidade de um recurso computacional, como um serviço, um computador ou uma rede conectada à Internet. Em um ataque de negação de serviço, um atacante com motivação financeira, política ou puramente destrutiva interrompe o serviço de uma vítima adicionando uma carga excessivamente alta de tráfego ao(s) serviço(s) da vítima [Rossow 2014]. DoS é comumente alcançado por meio do esgotamento de recursos, como no lado do servidor enviando mais solicitações do que ele pode manipular [Jonker et al. 2017].

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

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

Os ataques DDoS continuam a se tornar cada vez mais devastadores. Em Agosto de 2021, Microsoft registrou e anunciou uma largura de banda de 2.4 Terabits por segundo de ataque distribuído de negação de serviço mitigados contra Azure Cloud Service, O maior ataque DDoS até o momento registrado pela compania [Rangapur et al. 2022].

Os atacantes podem incrementar seus ataques estruturando-os para utilizarem refletores. Para um atacante, um refletor é qualquer nó na rede que envia dados para um IP em resposta a uma requisição recebida anteriormente. Refletores podem amplificar a quantidade de dados enviados, ou seja, sua resposta produz mais bytes ou pacotes, ou ambos, do que a requisição recebida. Assim, refletores potencializam o tráfego gerado por um atacante [Gondim et al. 2020]. Esse tipo de ataque é chamado de ataque distribuído de negação de serviço por reflexão (*Distributed Reflection Denial of Service*, DRDoS). Em um ataque DRDoS geralmente são usados servidores de comando e controle C&C *(Command and Control)*, *bots* e refletores na rede, conforme ilustrado na Figura 1.

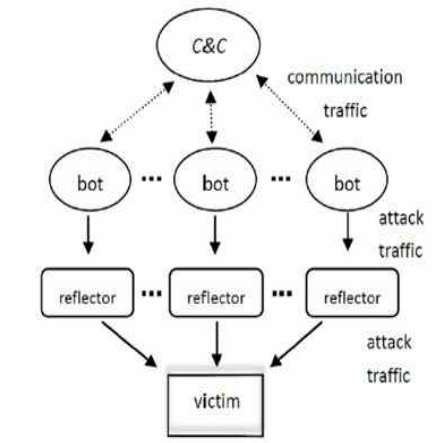

Figura 1. Estratégia de ataque DRDoS [Alieyan et al. 2016].

O fluxo apresentado na Figura 1, acontece com o atacante em total poder dos servidores de comando e controle (C&C), que são capazes de instruir os *bots* a enviarem requisições para um ou mais refletores utilizando o endereço de IP do alvo *(victim)* como endereço de origem, levando os refletores infectados a acreditar que a origem das requisições é a vítima, e assim enviar as respostas para essa. Dessa forma, um grande volume de dados chega a vítima pelos refletores sempre que uma conexão com a vítima for estabelecida [Alieyan et al. 2016]. Portanto, enquanto a vítima estiver sob ataque, ela poderá sofrer saturação da rede e elevação no consumo de recursos de processamento, memória e armazenamento, com consequente indisponibilidade de serviços.

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

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

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

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

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

Esse documento está organizado da seguinte forma, na Seção 2 de fundamentação teórica são apresentados os conceitos básicos de ataques DRDoS, *honeypots* e uma linha do tempo apresentando dados relevantes sobre ataques de negação de serviço ao longo do tempo. A Seção 3 aborda os trabalhos relacionados na literatura. Na Seção 4 é apresentado a proposta desse trabalho de preencher uma lacuna da literatura. Por fim, a Seção 5 apresenta um panorama do trabalho e aborda os problemas de pesquisa e demarca os próximos passos referentes a proposta.

2. Fundamentação Teórica

Este seção faz uma revisão dos conceitos necessários ao entendimento deste trabalho baseado na literatura já existente. A Seção 2.1 apresenta fundamentos de ataques DRDoS. A

Seção 2.2 aborda conceitos e funcionalidades de *honeypots*. A Seção 3 expõe os trabalhos relacionados mais recentes encontrados na literatura.

2.1. Ataques Distribuídos de Negação de Serviço por Reflexão (DRDoS)

Um ataque distribuído de negação de serviço (DDoS) é projetado para sobrecarregar as vítimas com tráfego e impedir que seus recursos de rede funcionem corretamente para seus clientes legítimos. Os ataques DDoS exigem uma quantidade significativa de largura de banda para atacar com sucesso um grande adversário [Nazario 2008]. O modelo tradicional de um ataque DDoS, é onde alguém cria ou contrata um *botnet* que é uma coleção de milhares de PCs de usuários comuns que foram infectados com *malware* para direcionar grandes quantidades de tráfego de rede para um único alvo [Mansfield-Devine 2015].

Um tipo de ataque DDoS são os ataques distribuídos de negação de serviço por reflexão (DRDoS) (também conhecidos como ataques DDoS de amplificação), nos quais o tráfego é encaminhado através de serviços intermediários desavisados, conhecidos como refletores [Paxson 2001]. Os ataques DRDoS não apenas dificultam a atribuição devido a uma camada extra de indireção, mas também fornecem amplificação de tráfego, facilitando a geração de tráfego suficiente para interromper o alvo, especialmente quando vários refletores são usados simultaneamente [Heinrich et al. 2021].

Um ataque DRDoS se difere de ataques DDoS pela sua camada extra de amplificação conforme apresentado na Figura 2. Na figura um atacante deseja indisponibilizar serviços esgotando a largura de banda da vítima no caso de ataques DDoS (parte superior da figura), apenas uma camada de *Bots* é utilizada para distribuir requisições e atacar a vítima. Já na parte inferior (DRDoS) ataques distribuídos utilizam reflexão com uma camada extra de amplificação que pode infringir mais danos ainda à vítima do que utilizando apenas *Bots*.

Ataques de negação de serviço são conhecidos há muito tempo, e ataques DDoS vêm ocorrendo na Internet há cerca de 25 anos e tiveram muitas evoluções ao longo desse período. A Tabela 1 retrata a evolução desses ataques apresentando eventos importantes que aconteceram desde 1974. A finalidade é apresentar qual o impacto que os ataques obtiveram ao decorrer dos anos e quais os métodos explorados para a sua realização [V. Revuelto 2017].

Em um ataque distribuídos de negação de serviço por reflexão (*distributed reflection denial of service*, 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*. Um atacante tem como objetivo esgotar a largura de banda da vítima. Ele abusa do fato de que servidores públicos de protocolos de rede baseados em UDP respondem a solicitações sem validar mais a identidade (ou seja, o endereço IP) do remetente [Rossow 2014]. É importante destacar que os refletores não são controlados pelo atacante, mas sistemas vulneráveis ou mal configurados que são abusados para a realização de ataques [Heinrich 2019].

Os ataques DRDoS exploram softwares maliciosos (*malware*) para controlar um grande número de conjuntos de bots, formando *botnets*, e comandam essas *botnets* para enviar requisições aos refletores, falsificando os endereços IP de origem para o usuário alvo [Chen et al. 2020]. Os refletores então ao receberem requisições com o IP de origem forjado, enviam as respostas para a vítima.

Tabela 1. Linha temporal de ataques de negação de serviço

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

Fonte: Adaptado de [Heinrich 2019]

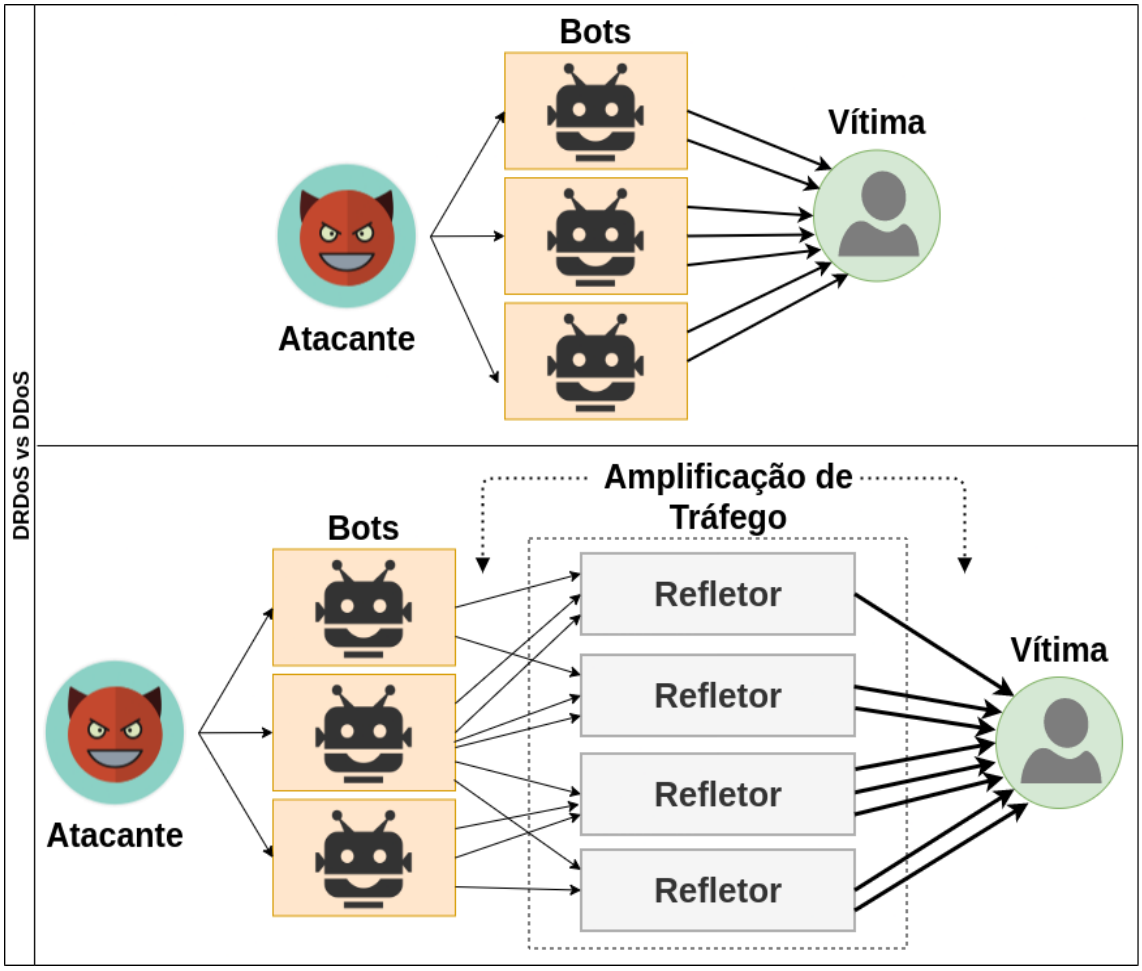

Figura 2. Ataques Distribuídos de Negação de Serviço vs Ataques Distribuídos de Negação de Serviço por Reflexão. Adaptado de [Heinrich 2019].

Ataques DRDoS oferecem aos atacantes vários benefícios, mas os principais são [Rossow 2014]:

1. Ele disfarça sua identidade, pois as vítimas recebem tráfego de amplificadores, ou seja, sistemas que podem ser abusados para enviar tráfego para a vítima em nome do atacante;
2. O abuso simultâneo de múltiplos amplificadores permite que um ataque DoS altamente distribuído seja conduzido a partir de um único *uplink* na Internet;
3. O tráfego refletido para a vítima é significativamente maior em largura de banda do que o tráfego que um atacante tem que enviar aos amplificadores.

Múltiplos protocolos podem ser utilizados para amplificar ataques de negação de serviço. A maioria são protocolos de aplicação que usam UDP como protocolo de transporte, mas existem também ataques por reflexão usando protocolos como ICMP e TCP. Diversos fatores influenciam a popularidade dos protocolos, principalmente o fator de amplificação alcançado e a disponibilidade de refletores abertos na Internet [Heinrich 2019]. Esses refletores são geralmente servidores vulneráveis ou mal configurados que são abusados em ataques de negação de serviço.

A amplificação desses protocolos é o principal fator na escolha dos atacantes, pois isso significa que a partir de N bytes enviados aos refletores, o protocolo/serviço em questão irá multiplicar essa quantidade de bytes de suas requisições pelo fator de amplificação de cada protocolo:

- NTP - Fator amplificação 556.9 [Czyz et al. 2014];
- SSDP - Fator amplificação 30.8 [Majkowski 2017];
- Chargen - Fator amplificação 358.8 [Rossow 2014];
- QOTD - Fator amplificação 140.3 [CERT 2014];
- Steam - Fator amplificação 5.5 [CERT 2014];
- DNS - Fator amplificação 28-54 [C. 2016];
- Memcached - Fator amplificação 10.000-51.000 [Newman 2018, Bai 2018];
- SNMP - Fator amplificação 6.3 [BITAG 2012];
- HTTP - Fator amplificação 79-100 [Beckett and Sezer 2017];
- CLDAP - Fator amplificação 33-70 [Choi and Kwak 2017];
- LDAP - Fator amplificação 46-55 [CERT 2014].

2.2. Honeypots

Honeypots são sistemas de isca utilizados na rede para atrair invasores e atacantes para que eles utilizem esse sistema e as atividades realizadas por esses atacantes sejam capturadas para uma análise futura [Bhagat and Arora 2018]. *Honeypots*, por sua natureza, não são criados para serem acessados por usuário legítimos e sim com o objetivo de serem sondados, atacados ou até mesmo comprometidos [Hoepers et al. 2007]. Dessa forma, *honeypots* são extensivamente monitorados para possibilitar o estudo do comportamento e das atividades dos atacantes, levando à descoberta de novos ataques e de como ataques já conhecidos na teoria são realizados na prática [Heinrich 2019]. No caso de ataques DRDoS *honeypots* são utilizados como refletores pelos atacantes para amplificar os ataques de negação de serviço.

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

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

Entre os *honeypots* de alta e baixa interatividade tem o de média interatividade que possuem alguns protocolos e serviços que são emulados ou seja, o próprio *honeypot* gera as respostas, que podem ser fixas ou dependentes da requisição assim não havendo qualquer interação com servidores reais. Os outros serviços que são intermediados o *honeypot* funciona como um *proxy* que repassa a requisição para que um servidor real processe, e encaminha a resposta do servidor de volta para a origem.

Honeypots de alta interatividade possuem mais interações e então tendem a receber uma maior quantidade de requisições e consequentemente recolher uma maior quantidade de *payload* que os de baixa interatividade. Um *honeypot* de média interatividade é o MP-H (originalmente HReflector) [Heinrich 2019, Heinrich et al. 2021] um *honeypot* que suporta múltiplos protocolos baseados em UDP. Outro exemplo de *honeypot* de média interatividade é o AmpPot [Krämer et al. 2015] que teve a sua arquitetura utilizada como base para o desenvolvimento do MP-H.

O *honeypot* do MP-H que será utilizado nesse trabalho tem o seu fluxo de funcionamento conforme apresentado na Figura 3 em que uma requisição enviada por um atacante (1) chega ao *honeypot* e é contabilizada (2). O *honeypot* então consulta o endereço IP de origem na *blacklist* para decidir se uma resposta deve ou não ser enviada. Caso negativo, o processamento da requisição encerra (3). Caso afirmativo, o *honeypot* produz uma resposta para a requisição (4), de modo fixo para os protocolos Chargen, NTP, QOTD, SSDP, CoAP, CLDAP e Steam e funcionando como um *proxy* para os protocolos DNS e Memcached. A resposta obtida é então enviada para o cliente, que pode ser uma vítima (no caso de ataque por reflexão) ou o próprio atacante quando este envia *probes* para o *honeypot*. O passo 6 representa a coleta de tráfego (*payloads*) com o Tcpdump, o passo 7 a limpeza periódica das tabelas *hash* em memória, com armazenamento persistente dos dados relevantes para análise posterior em um banco de dados, e o passo 8 representa a compressão das informações capturadas pelo Tcpdump [Heinrich 2019].

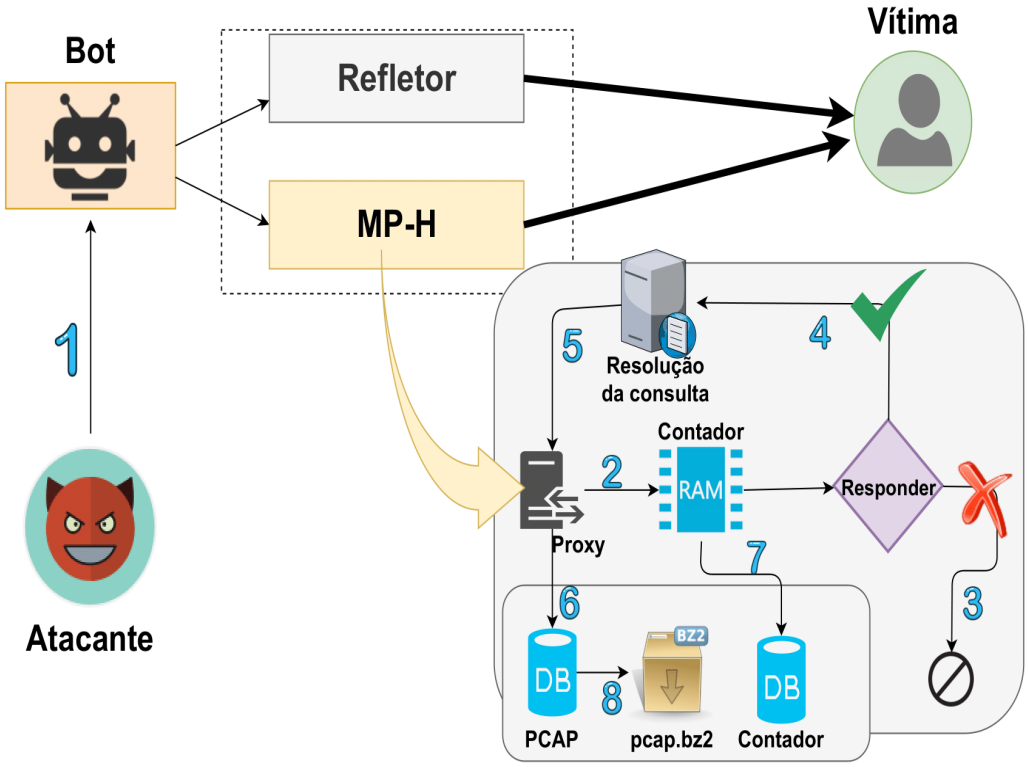

Figura 3. Fluxo de processo de requisições do MP-H [Heinrich 2019].

O objetivo de expor o *honeypot* como um endereço público aberto é receber os ataques, e armazenar informações sobre eles, como quantidade de dados enviados e retornados, endereços IP e portas de origem e destino, e conteúdo das requisições e respostas

(*payloads*). Quando um *honeypot* é usado como refletor em um ataque DRDoS, o endereço IP de origem corresponde à vítima, e não ao atacante, devido ao uso de IP *spoofing*.

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

3. Trabalhos Relacionados

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

- Evolução temporal de ataques [Ryba et al. 2015, Deka et al. 2017] com o auxílio da análise de *payloads*;
- Captura de *payloads* utilizando *honeypots* [Heinrich et al. 2021, Krämer et al. 2015, Zhauniarovich and Dodia 2019];
- Análise de *payload* para detecção de ataques DRDoS [Xu et al. 2019, Heinrich 2019, Dahiya et al. 2020]

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

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

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

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

[Thomas et al. 2017] executou uma análise de *payload* do tráfego DRDoS coletado de um grande conjunto de *honeypots* UDP para oito protocolos (QOTD, Chargen, DNS, NTP, SSDP, MS-SQL, Portmap e mDNS). A pesquisa observou mais de 5,8 milhões de ataques em um período de 1010 dias e analisou o comportamento de varredura e

várias características de ataque (duração, contagem de pacotes, número de ataques). NTP e DNS foram os protocolos mais populares, mas também notaram quantidades significativas de tráfego SSDP.

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

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

Após analisar e documentar todos os trabalhos relacionados é possível apresentar todos eles em uma tabela comparando quais protocolos foram implementados pelos *honeypots*, qual o número de *honeypots* implantados para realizar a pesquisa e o período em que os *honeypots* implantados permaneceram ativos para a coleta de *payloads* conforme a Tabela 3.

Referência	Protocolos	Número de Honeypots	Período de coleta de dados
[Rossow 2014]	NTP, SNMP, SSDP, NetBios, CharGen, QOTD, P2P, BitTorrent, Quake 3, Steam, DNS, Kad, ZAv2, Sality e Gameover	1	12 dias
[Krämer et al. 2015]	NTP, DNS, Chargen, SSDP, MS-SQL, NetBIOS, QOTD, SIP e SNMP	21	121 dias
[Noroozian et al. 2016]	NTP, DNS, Chargen, SSDP, QOTD e SNMP	8	730 dias
[Thomas et al. 2017]	QOTD, Chargen, DNS, NTP, SSDP, MS-SQL, Portmap e mDNS	65	1010 dias
[Jonker et al. 2017]	NTP, DNS, CharGen, SSDP e RIPv1	24	731 dias
[Heinrich et al. 2021]	Chargen, DNS, NTP, Memcached, QOTD, SSDP, CoAP, CLDAP e Steam	1	731 dias

Tabela 2. Resumo dos trabalhos relacionados.

Enquanto esses estudos analisam os *payloads* para investigar, caracterizar e predizer ataques distribuídos de negação de serviço, eles praticamente ignoram a evolução

do conteúdo desses *payloads* de ataques ao longo do tempo. Na verdade, [Rossow 2014] observa e analisa o tamanho dos *payloads* em quantidades de bytes para definir o fator de amplificação de largura de banca e também para defender e filtrar ataque de pacotes que contenham o *payload* idêntico ou próximo, contudo não chegam a analisar como o conteúdo ou tamanho do *payload* desses ataques muda com o tempo. O diferencial desse trabalho, portanto, reside na investigação de análise temporal de evolução de *payloads* utilizados em ataques DRDoS.

4. Proposta

Esse trabalho busca estender o trabalho apresentado por [Heinrich et al. 2021], com o foco em análise de *payloads*. Após a análise dos trabalhos relacionados, pode-se destacar algumas lacunas na literatura como questões relacionadas com a análise dos dados (*payloads*) recolhidos pelos *honeypots*.

Uma das questões que não são apresentadas na literatura é a comparação e correlação dos *payloads* entre dois ou mais *honeypots*. Os *payloads* observados e coletados por diferentes *honeypots* são similares, ou possuem diferenças entre eles? Por exemplo, considerando dois ou mais honeypots que suportem um protocolo em comum, como DNS, e que tenham coletado dados em um mesmo período, em quais aspectos os payloads recebidos diferem e em quais se assemelham?

Outra questão é a falta de análise longitudinal da evolução dos *payloads* de ataques de negação de serviço ao longo do tempo. Por exemplo, o *honeypot* MP-H (originalmente HReflector) [Heinrich 2019, Heinrich et al. 2021] iniciou a coletar dados em setembro de 2017 e até o momento continua com seus *honeypots* ativos, apresentando assim mais de 300GB de dados em arquivos PCAP e suporte a 7 protocolos que podem ser analisados em termos de quais mudanças e evoluções ocorreram no ataques que abusavam dos diferentes protocolos nos últimos 5 anos.

Existem diversos fatores que podem levar à evolução dos *payloads*. Por exemplo, estudos anteriores mostraram que ataques DRDoS usando DNS usavam majoritariamente consultas do tipo ANY, que eram capazes de induzir fatores de amplificação próximos a 100 [Fachkha et al. 2015, Heinrich 2019, Heinrich et al. 2021]. Isso levou a mudanças na especificação do DNS para modificar o processamento de consultas ANY, com vistas a coibir o seu uso em ataques por reflexão [RFC 8482]; será que essa alteração (formalizada em 2019, mas que já vinha sendo discutida desde 2015) levou a uma adaptação por parte dos atacantes? Outro fator que pode provocar evolução é a descoberta de variantes de ataques, como ataques *slow drip* [Urban and Burton 2019]; será que essas novas variantes passaram a ser usadas? Quanto tempo depois de terem sido discutidas publicamente?

A infraestrutura do MP-H iniciou-se com apenas um *honeypot* ativo na infraestrutura disponibilizada pela UDESC. Ao longo do tempo, outros *honeypots* foram implantados e no momento existem três dispositivos com *honeypots* ativos e recolhendo dados. Esses *honeypots* estão distribuídos da seguinte maneira:

- Dois honeypots na rede da UDESC:
  - Um *honeypot* ativo desde setembro de 2017;
  - Um *honeypot* ativo desde agosto de 2021;
  - Protocolos: Chargen, DNS, Memcached, NTP, QOTD, SSDP e Steam;

- Um *honeypot* na rede da UFPR:
  - Um *honeypot* ativo desde setembro de 2021;
  - Protocolos: Chargen, DNS, Memcached, NTP, QOTD, SSDP e Steam;

A proposta deste trabalho de mestrado é preencher as lacunas encontradas na literatura, usando os dados coletados pelas várias instâncias do *honeypot* MP-H para:

1. Realizar uma análise longitudinal da evolução dos *payloads*, considerando os diferentes protocolos implementados pelo MP-H;
2. Comparar os *payloads* recebidos pelas diferentes instâncias.

Dessa forma, a pesquisa envolverá as etapas de analisar o conteúdo recolhidos pelos *honeypots* em arquivos PCAP, o tamanho de todo o *dataset* recolhido e quais protocolos foram mais abusados. Seguido pela etapa minuciosa de análise dos *payloads* e então um período para realizar a análise longitudinal e outro para fazer a comparação entre diferentes *honeypots* e um intervalo para realizar o desenvolvimento de um artigo para publicação e por fim um período para escrever a dissertação conforme apresentado na Tabela 4

Etapa	Data de início	Data de finalização
Analisar conteúdo recolhido pelos *honeypots*	28/02	13/03
Análise dos *payloads*	14/03	27/03
Análise longitudinal	28/03	24/04
Comparação entre *honeypots*	25/04	29/05
Desenvolvimento de artigo	30/05	26/06
Escrever a dissertação	27/06	31/08

Tabela 3. Etapas a serem concluídas para finalizar o mestrado.

5. Conclusão

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

Além de realizar a análise longitudinal de evolução dos *payloads*, esse projeto de mestrado intende analisar e comparar dados (*payloads*) recolhidos por dois ou mais *honeypots*. As comparações a serem realizadas em relação ao período em que foram recolhidos pode-se analisar os *payloads* que tiverem intersecção do período em que foram coletados. Dados coletados em períodos e de *honeypots* diferentes também podem ser analisados e correlacionados.

Este trabalho propõe investigar *payloads* de ataques DRDoS de que são coletados por *honeypots*, uma ferramenta útil para compreender o funcionamento de ataques e acompanhar a evolução das técnicas usadas pelos atacantes que armazena as requisições recebidas, esses *honeypots* recebem as requisições dos atacantes através dos refletores coletam as informações em arquivos PCAP. Os *payloads* a serem analisados são os arquivos PCAP extraídos de três instâncias do *honeypot* MP-H, sendo duas instaladas na rede da UDESC e uma na rede da UFPR.

Referências

Adamsky, F., Khayam, S. A., Jäger, R., and Rajarajan, M. (2015). P2P file-sharing in hell: Exploiting BitTorrent vulnerabilities to launch distributed reflective DoS attacks. In *9th USENIX Workshop on Offensive Technologies (WOOT 15)*, Washington, D.C. USENIX Association.

Alieyan, K., Kadhum, M. M., Anbar, M., Rehman, S. U., and Alajmi, N. K. (2016). An overview of DDoS attacks based on DNS. In *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 276–280. IEEE.

Bai, K. (2018). Analysis and Prevention of Memcache UDP Reflection Amplification Attack. *International Journal of Science*, 5(3):297–302.

Beckett, D. and Sezer, S. (2017). Http/2 tsunami: Investigating http/2 proxy amplification ddos attacks. In *2017 Seventh International Conference on Emerging Security Technologies (EST)*, pages 128–133. IEEE.

Bhagat, N. and Arora, B. (2018). Intrusion detection using honeypots. In *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pages 412–417. IEEE.

Bienkowski, T. (2018). No sooner did the ink dry: 1.7 TBps DDoS attack makes history.

BITAG (2012). Snmp reflected amplification ddos attack mitigation. *SNMP Reflected Amplification DDoS Attack Mitigation (August 1, 2012)*.

Brewster, T. (2013). Cyber attacks strike Zimbabweans around controversial election.

C., H. (2016). Recomendações para evitar o abuso de servidores dns recursivos abertos. `https://www.cert.br/docs/whitepapers/dns-recursivo-aberto/`. (Accessed on 02/12/2022).

CERT (2014). Udp-based amplification attacks | cisa. `https://www.cisa.gov/uscert/ncas/alerts/TA14-017A`. (Accessed on 02/12/2022).

CERT, S. A. (1998). Cert: http://www.cert.org/advisories. Technical report, CA-1998-01. html.

CERT.br (2016). Recomendações para melhorar o cenário de ataques distribuídos de negação de serviço (DDoS). *https://www.cert.br/docs/whitepapers/ddos/*.

Chen, X., Feng, W., Ma, Y., Ge, N., and Wang, X. (2020). Preventing DRDoS attacks in 5G networks: a new source IP address validation approach. In *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pages 1–6. IEEE.

Choi, S.-J. and Kwak, J. (2017). A study on reduction of ddos amplification attacks in the udp-based cldap protocol. In *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, pages 1–4. IEEE.

Cornell (1984). 18 U.S. Code § 1030 - fraud and related activity in connection with computers | U.S. code | US law | lii / legal information institute.

Cox, J. (2014). The history of DDoS attacks as a tool of protest. `https://www.vice.com/en/article/d734pm/history-of-the-ddos-attack`. (Accessed on 01/09/2022).

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

Dahiya, A., Joshi, K., Nandal, R., Yadav, R., and Gupta, S. B. (2020). Honeynet based defensive mechanism against DDoS attacks. *International Journal of Information Security Science*, 9(3):140–153.

Dear, B. (2010). Perhaps the first denial-of-service attack. *PLATO History Blog*.

Deka, R. K., Bhattacharyya, D. K., and Kalita, J. K. (2017). DDoS attacks: Tools, mitigation approaches, and probable impact on private cloud environment. *Big Data Analytics for Internet of Things*, pages 285–319.

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

Gondim, J. J., de Oliveira Albuquerque, R., and Orozco, A. L. S. (2020). Mirror saturation in amplified reflection distributed denial of service: A case of study using SNMP, SSDP, NTP and DNS protocols. *Future Generation Computer Systems*, 108:68–81.

Haque, M. R., Tan, S. C., Yusoff, Z., Nisar, K., Kaspin, R., Haider, I., Nisar, S., Rodrigues, J. J., Shankar Chowdhry, B., Uqaili, M. A., et al. (2022). Unprecedented smart algorithm for uninterrupted SDN services during DDoS attack. *Computers, Materials & Continua*, 70(1):875–894.

Heinrich, T. (2019). Caracterização de ataques DRDoS usando *honeypot*. Master's thesis, Dissertação de mestrado em Computação Aplicada, Universidade do Estado de Santa Catarina - UDESC, Joinville (SC).

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

Hoepers, C., Jessen, K. S., and Chaves, M. (2007). Honeypots e honeynets: Definições e aplicações. *Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, ver*.

Husák, M. and Vizváry, M. (2013). Poster: Reflected attacks abusing honeypots. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 1449–1452.

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

Khandelwal, S. (2016). World's largest 1Tbps DDoS attack launched from 152,000 hacked smart devices. *The Hacker News*.

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

Lemos, R. (2018). History shows DDoS volumes to keep rising despite mitigation efforts. https://www.eweek.com/security/how-ddos-attacks-techniques-have-evolved-over-past-20-years/. (Accessed on 01/09/2022).

Lopes, R. W. (2015). Ataques DDoS panorama, mitigação e evolução. https://ftp.registro.br/pub/gter/gter39/08-AtaquesDdosPanoramaMitigacaoEvolucao.pdf. (Accessed on 01/09/2022).

Majkowski, M. (2017). (Accessed on 02/12/2022).

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

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

Newman, L. H. (2018). Github survived the biggest DDoS attack ever recorded. *Wired*, 1.

NIST (1999). Nvd - cve-1999-1379. https://nvd.nist.gov/vuln/detail/CVE-1999-1379. (Accessed on 01/09/2022).

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

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

Prince, M. (2013). The DDoS that almost broke the internet. https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/.

Prolexic (2013). Distributed reflection denial of service (DRDoS) attacks an introduction to the DRDoS white paper series. https://news.asis.io/sites/default/files/Distributed_Reflection_DoS_Attacks_White_Paper_A4_031513.pdf. (Accessed on 11/09/2021).

Rangapur, A., Kanakam, T., and Jubilson, A. (2022). DDoSDet: An approach to detect DDoS attacks using neural networks. *arXiv preprint arXiv:2201.09514*.

Rossow, C. (2014). Amplification hell: Revisiting network protocols for DDoS abuse. In *NDSS*.

Ryba, F. J., Orlinski, M., Wählisch, M., Rossow, C., and Schmidt, T. C. (2015). Amplification and DRDoS attack defense–a survey and new perspectives. *arXiv preprint arXiv:1505.07892*.

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

Urban, A. and Burton, R. (2019). Characterizing certain DNS DDoS attacks. `https://indico.dns-oarc.net/event/32/contributions/722/attachments/694/1205/Urban_DDoSAttacks_DNS-OARC.pdf`. (Accessed on 02/07/2022).

V. Revuelto, S. Meintanis, K. S. (2017). DDoS overview and response guide. `https://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf`. (Accessed on 01/31/2022).

Welzel, A., Rossow, C., and Bos, H. (2014). On measuring the impact of DDoS botnets. In *Proceedings of the Seventh European Workshop on System Security*, pages 1–6.

Woody, C., Mead, N., and Shoemaker, D. (2012). Foundations for software assurance. In *2012 45th Hawaii International Conference on System Sciences*, pages 5368–5374. IEEE.

Xu, R., Cheng, J., Wang, F., Tang, X., and Xu, J. (2019). A DRDoS detection and defense method based on Deep Forest in the Big Data environment. *Symmetry*, 11(1):78.

Zetter, K. (2009). Lazy hacker and little worm set off cyberwar frenzy. *Wired News. http://www. wired. com/threatlevel/2009/07/mydoom*.

Zhauniarovich, Y. and Dodia, P. (2019). Sorting the garbage: filtering out DRDoS amplification traffic in ISP networks. In *2019 IEEE Conference on Network Softwarization (NetSoft)*, pages 142–150. IEEE.