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

ANTEPROJETO DE PESQUISA

TEMA: SEGURANÇA, COMPUTAÇÃO PARALELA E DISTRIBUÍDA

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

RAFAEL TENFEN

JOINVILLE, 2022

RESUMO

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

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

ABSTRACT

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

Keywords: latex. abntex. text editoration.

SUMÁRIO

1 INTRODUÇÃO

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; CLAYTON; BERESFORD, 2017).

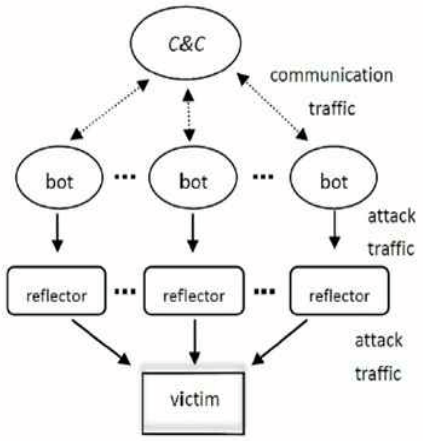
Ao ser atacado, o alvo de um ataque DDoS não consegue diferenciar os acessos legítimos ao sistema dos maliciosos e pode ficar sobrecarregado ao tentar tratar todas as requisições recebidas (CERT.BR, 2016). Uma maneira comum de iniciar ataques DDoS são *botnets* DDoS, ou seja, redes infectadas por *malware*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

Os ataques DDoS continuam a se tornar cada vez mais devastadores. Em Agosto de 2021, Microsoft registrou e anunciou uma largura de banda de 2.4 Terabits por segundo de ataque distribuído de negação de serviço mitigados contra Azure Cloud Service, O maior ataque DDoS até o momento registrado pela compania (RANGAPUR; KANAKAM; JUBILSON, 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; ALBUQUERQUE; OROZCO, 2020). Esse tipo de ataque é chamado de ataque distribuído de negação de serviço por reflexão (*Distributed Reflection Denial of Service*, DRDoS). Em um ataque DRDoS geralmente são usados servidores de

comando e controle C&C *(Command and Control)*, *bots* e refletores na rede, conforme ilustrado na Figura 1.

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



Fonte: (ALIEYAN et al., 2016)

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

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

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

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

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

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

1.1 PROPOSTA

1.2 ESTRUTURA DO DOCUMENTO

2 REVISÃO DE LITERATURA

Este capítulo faz uma fundamentação dos conceitos necessários ao entendimento deste trabalho baseado na literatura já existente. A Seção 2.1 apresenta fundamentos de ataques DRDoS. A Seção 2.2 aborda conceitos e funcionalidades de *honeypots*. A Seção 2.3 expõe os trabalhos relacionados mais recentes encontrados na literatura.

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

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

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

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

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

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

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

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

Tabela 1 Linha temporal de ataques de negação de serviço

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

Fonte: Adaptado de (HEINRICH, 2019)

2.2 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; ARORA, 2018). No caso de ataques DRDoS honeypots são utilizados como refletores pelos atacantes para amplificar os ataques de negação de serviço.

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

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

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

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

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

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

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

2.3 TRABALHOS RELACIONADOS

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

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

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

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

Krämer et al. (2015) realizou a introdução aos AmpPots, que são *honeypots* projetados para observar e coletar tráfego DRDoS usando nove protocolos (NTP, DNS, Chargen,

SSDP, MS-SQL, NetBIOS, QOTD, SIP e SNMP). Eles analisaram dados coletados de 21 AmpPots entre fevereiro e maio de 2015, totalizando mais de 1,5 milhão de ataques, e descreveram características como duração do ataque, geolocalização da vítima e entropia de solicitação com a análise de *payloads*. Também realizaram um análise de *botnets* DDoS.

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

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

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

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

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

utilizados em ataques DRDoS.

2.4 CONSIDERAÇÕES DO CAPÍTULO

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

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

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

3 PROPOSTA

3.1

Nosso problema é...

Infraestrutura do honeypot

dado nossa longa data com os honeypots vamos analisar o seguinte

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

4 ANÁLISE DE DADOS

Nessa sessão serão apresentados os

4.1 IMPLANTAÇÃO

4.2 OBSERVAÇÕES GERAIS

4.3 AVALIAÇÃO POR PROTOCOLO

4.3.1 NTP - *Network Time Protocol*

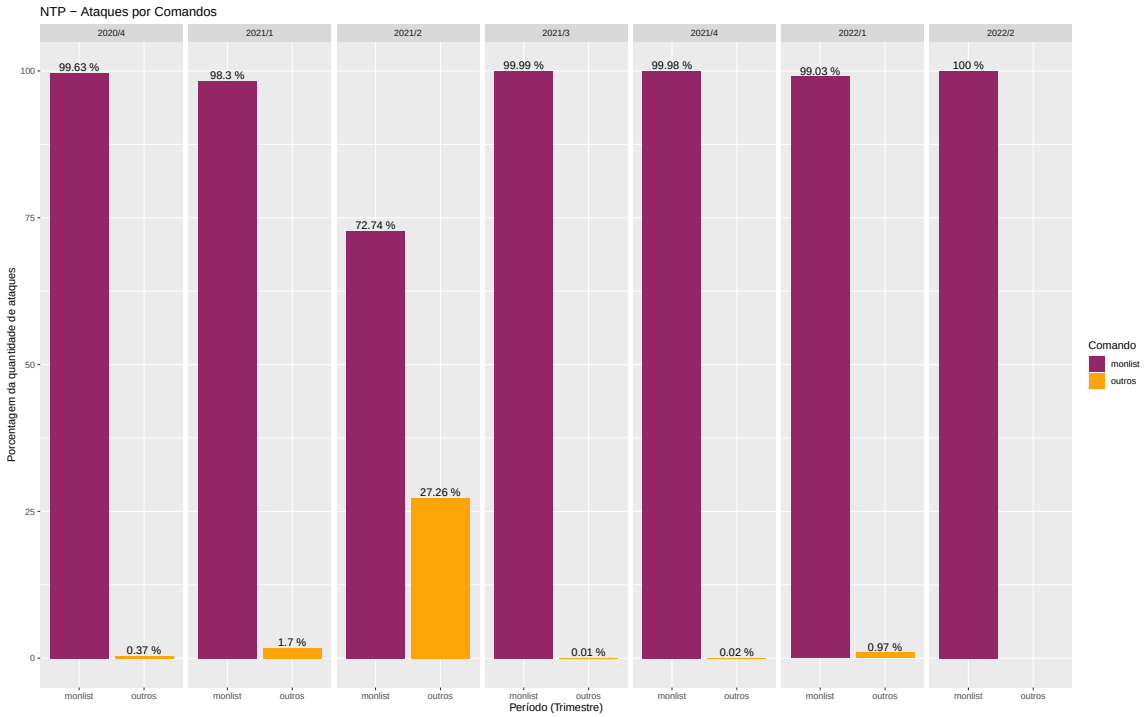
O objetivo principal do protocolo NTP é sincronizar o horário do sistema com o servidor. O atacante utiliza como endereço de IP de origem das requisições o IP da vítima, para que a resposta da requisição seja enviada para a vítima de modo amplificado. O comando `MONLIST` nos servidores NTP vem sendo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

Estudos anteriores mostraram um predomínio de requisições `MONLIST` em ataques DRDoS usando NTP: (HEINRICH, 2019) reportou que 99,9999% das requisições utilizadas em ataques NTP utilizaram o comando `MONLIST` em um período de 255 dias. A Figura 2 mostra a incidência de ataques com `MONLIST` em cada trimestre. Observa-se que houve mais de 99% de ataques usando `MONLIST` em todos os trimestres, com exceção de 2021/2, onde houve 27.26 % de outros ataques. Parte desse tráfego consiste em *payloads* de CLDAP e DNS na porta errada; 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 seguem a especificação, não correspondem a *payloads* de outros protocolos e para os quais não se encontrou uma explicação mesmo com análise manual.

4.3.2 DNS - *Domain Name System*

Servidores DNS são utilizados para traduzir domínios legíveis por humanos em endereços de IP. Por exemplo o domínio "www.amazon.com"para seu endereço de IP "192.0.2.44". Entretanto, uma das maneiras que atacantes utilizam esse protocolo protocolo é abusando do `QTYPE ANY` que comumente era utilizado para depurar os servidores DNS, pois retorna com detalhes sobre subdomínios, servidores de backup, servidores de e-mails, *aliases* e demais detalhes referentes ao domínio. O DNS é interessante a ataque de amplificação, devido a quantidade de bytes da resposta superar o tamanho da requisição.

Figura 2 – Incidência de `MONLIST` em ataques usando NTP



Fonte: Autor

Como o DNS usa por padrão o UDP as respostas do servidor são respostas legítimas, a qual dificulta a identificação entre os pacotes legítimos enviados por usuários autorizados ou por um atacante (CHEEMA et al., 2022).

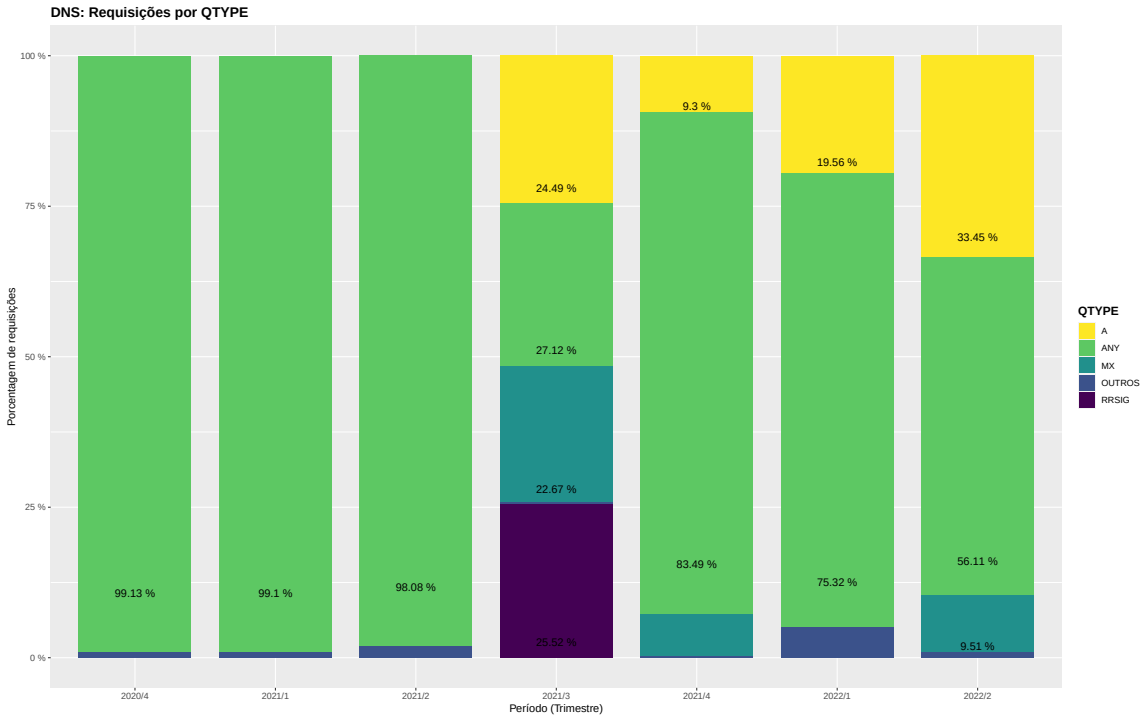
Servidores DNS armazenam informações sobre os domínios em `RR` que é um acrônimo para *Resource Records* (HOFFMAN; SULLIVAN; FUJIWARA, 2019). Em um servidor DNS um domínio identifica um nó. Cada nó possui um conjunto de informações, que podem estar vazios. O conjunto de informações associado a um nome específico é composto de vários registros de recursos (RRs). A ordem dos RRs em um conjunto não é significativa e não precisa ser preservada por servidores, resolvedores ou outras partes do DNS (MOCKAPETRIS, 1987).

Um servidor DNS possui implementações de `QTYPE` (pq tenho diferentes QTYPEs) diferentes como `MX`, `ANY` e outros. O `DNS MX` (troca de e-mails) RR foi inicialmente definido na RFC974 (PARTRIDGE, 1986) (é um roteamento de e-mails e sistema de domínios). Um domínio pode ter múltiplos `MX` RR e também cada RR de `MX` define a preferência ou prioridade de certo domínio (REED; REED, 2020). Já o DNS de `QTYPE ANY` em uma consulta é usado para retornar todos os RRs com mesmo QNAME, independente de seu QTYPE (HEINRICH, 2019). Assim realizando uma amplificação do tamanho da requisição para a resposta.

A Figura 3 mostra a porcentagem de requisições de ataques que utilizam DNS por `QTYPE` em cada trimestre. Observa-se que houve uma predominância nas requisições dos

ataques usando `ANY` em todos os trimestres, com exceção de 2021/3, onde foi observado uma alteração no comportamento com crescimento no uso de outros `QTYPE` nas requisições de ataques. Parte dessa disparidade é referente a uma falha no armazenamento de dados de DNS, afetando a quantidade de ataques nesse trimestre. Por exemplo no segundo trimestre de 2021 (2021/2) ocorreram 15.8 milhões de requisições em ataques DNS, já no terceiro trimestre (2021/3) 1.2 milhões de requisições, uma queda de 91.9% na quantidade de requisições de ataques DNS.

Figura 3 – Requisições DNS por `QTYPE`



Fonte: Autor

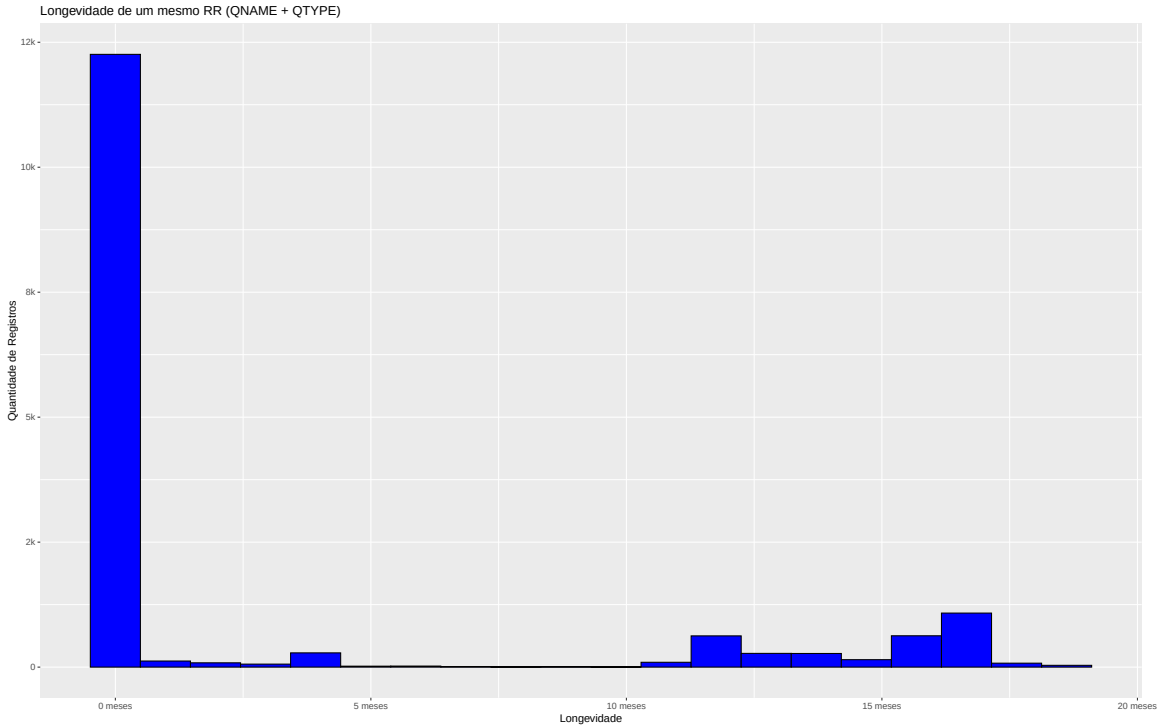
~~Uma das recomendações apresentadas na RFC8482 (ABLEY et al., 2019) é que o servidor `DNS` pode escolher não responder a consultas com o `QTYPE ANY` por razões de política local, motivados por segurança, desempenho ou outros motivos. O grande problema é que muitos servidores não seguem essa recomendação e disponibilizam esse recurso aos seus usuários e assim muitos atacantes continuam a abusar dessa técnica em ataques de amplificação.~~

~~A partir do terceiro trimestre de 2021 (2021/3), a quantidade de requisições de ataques DNS do `QTYPE A` vem crescendo~~. Considerando as observações é possível apontar que, QTYPE são RR ataques com alta longevidade, ou seja, o mesmo RR é utilizado em múltiplos ataques por um longo período de tempo (mais de 10 meses). Cerca de 79.5% de todos os ataques de alta longevidade utilizam o `QTYPE A`.

Na literatura não é encontrado abordagens apresentação de dados referentes a longevidade de RR *Resource Records* em ataques DNS. A longevidade de um RR `(QNAME+QTYPE)`

é definido como o intervalo entre a primeira e a última aparição desse RR em ataques. As observações encontradas focam em apresentar quanto tempo um mesmo domínio recebe ataques continuamente, por exemplo o `QNAME` "peacecorps.gov."do `QTYPE ANY` teve o primeiro ataque registrado em 31/10/2020 e o ultimo ataque com o mesmo `QNAME` e `QTYPE` em 11/05/2022 totalizando uma longevidade de aproximadamente um ano e meio (48 milhões de segundos) totalizando cerca de 118.333 ataques diferentes nesse período. A Figura 4 apresenta a longevidade de RR em meses, em que 12.014 (74.51%) RR tem uma baixa longevidade de até 1 dia de duração, apenas 863 (5%) RR receberam ataques com duração ente 1 dia e 10 meses e mais de 3.246 (20%) dos RR possuem uma alta longevidade com mais de 10 meses de duração.

Figura 4 – Longevidade de RR Resource Records em ataques DNS



Fonte: Autor

Observou-se que alguns domínios continuam a ser utilizados em ataques de amplificação e assim aumentando a sua longevidade, em (HEINRICH, 2017) na Tabela 4.14 dos top 15 domínios mais utilizados, 4 deles continuam ativos e utilizados em ataques DRDoS. Além disso, em (HEINRICH, 2019) na Tabela 17 dos 5 domínios apresentados 2 ainda estão ativos e continuam sendo utilizando em ataques.

O servidor DNS deve ser paranoico ao formar as respostas. Pois ele também deve verificar que a resposta é compatível com a requisição recebida utilizando o campo `TxID` na resposta. A resposta do DNS deve ser aceita somente se os seguintes requisitos forem aceitos:

- A seção da requisição do pacote de resposta é equivalente à de um pacote de requisição que está esperando por uma resposta.
- O campo ID (`TxID`) da resposta é equivalente ao ID da requisição.
- A resposta vem do mesmo endereço de rede de qual a requisição foi enviada.
- A resposta vem do mesmo endereço de rede, incluindo o número da porta em que a requisição foi enviada.

Em geral, a primeira resposta que satisfaz esses 4 requisitos deve ser aceita (HUBERT; MOOK, 2009).

O `TxID` no DNS é um número inteiro de 16 bits, o que significa que se utilizar todo os bits possíveis, e se o conteúdo desse campo é de fato randômico, vai necessitar na média 32768 tentativas para acertar o número correto (HUBERT; MOOK, 2009). Contudo, o campo `TxID` é um inteiro de 16 bits, então utilizando um método sequencial existem no máximo 2^16 possibilidades de preencher esse campo (0-65535). Entretanto, foi observado que vários ataques utilizavam o mesmo `TxID`, como apresentado na Tabela 2 em que o top 5 `TxID` que mais repetiram em requisições de um mesmo domínio, então para o "17767"de domínio "isc.org."em 2.65 milhões de requisições eram esperados uma repetição de `TxID` no máximo (sequencial 16 bits) 40 vezes ou até 80 vezes segundo a probabilidade apresentada na RFC5452, contudo entre todas as requisições o `TxID` repetiu 58.001 vezes.

Tabela 2 – Repetições de TxID em ataques DNS

TxID	**QNAME**	**Requisições**	**Repetição Observada**	**Repetição Esperada**
17767	isc.org.	2.65 M	58.001	40
26566	peacecorps.gov.	9 M	40.940	137
17767	sl.	6 M	29.801	90
1	pizzaseo.com.	331 k	6.442	5
13551	VERSION.BIND.	6 k	2.335	0

Fonte: Autor

Além da repetição do `TxID` em um mesmo domínio, é incomum observar múltiplos domínios utilizando o mesmo `TxID`. Como o `TxID` de número "17767"que foi utilizado em 87.924 ataques de DNS totalizando 9.063.853 requisições com o mesmo `TxID` entre cerca de 30 domínios diferentes. Isso levantou uma dúvida do porque tantos ataques utilizando o mesmo ID de referência.

Além do grande número de ataques utilizando o mesmo `TxID` e também a sobreposição entre os ataques sendo executados em um mesmo período sugerem que muitos deles utilizaram a mesma ferramenta para realizar os ataques. Pois os atacantes não realizaram

o trabalho de alterar o `TxID` ou utilizar um número randômico ou incremental para que o `TxID` fosse diferente entre seus ataques.

4.3.3 Memcached

5 CONCLUSÃO

REFERÊNCIAS

ABLEY, J. et al. *Providing minimal-sized responses to DNS Queries That Have QTYPE= ANY*. [S.l.], 2019. Citado na página 16.

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

BHAGAT, N.; ARORA, B. Intrusion detection using honeypots. In: IEEE. *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*. [S.l.], 2018. p. 412–417. Citado na página 9.

BIENKOWSKI, T. *No sooner did the ink dry: 1.7 tbps DDoS attack makes history*. [S.l.]: March, 2018. Citado na página 8.

BREWSTER, T. *Cyber Attacks Strike Zimbabweans Around Controversial Election*. [S.l.]: August, 2013. Citado na página 8.

CERT, S. A. *CERT: http://www. cert. org/advisories*. [S.l.], 1998. Citado na página 8.

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

CHEEMA, A. et al. Prevention techniques against distributed denial of service attacks in heterogeneous networks: A systematic review. *Security and Communication Networks*, Hindawi, v. 2022, 2022. Citado 2 vezes nas páginas 14 e 15.

CHEN, X. et al. Preventing drdos attacks in 5g networks: a new source ip address validation approach. In: IEEE. *GLOBECOM 2020-2020 IEEE Global Communications Conference*. [S.l.], 2020. p. 1–6. Citado na página 7.

CORNELL. *18 U.S. Code § 1030 - Fraud and related activity in connection with computers | U.S. Code | US Law | LII / Legal Information Institute*. 1984. Disponível em: <https://www.law.cornell.edu/uscode/text/18/1030>. Citado na página 8.

COX, J. *The History of DDoS Attacks as a Tool of Protest*. 2014. <https://www.vice.com/en/article/d734pm/history-of-the-ddos-attack>. (Accessed on 01/09/2022). Citado na página 8.

DAHIYA, A. et al. Honeynetbased defensive mechanism against ddos attacks. *International Journal of Information Security Science*, v. 9, n. 3, p. 140–153, 2020. Citado na página 10.

DEAR, B. Perhaps the first denial-of-service attack. *PLATO History Blog*, 2010. Citado na página 8.

DEKA, R. K.; BHATTACHARYYA, D. K.; KALITA, J. K. Ddos attacks: Tools, mitigation approaches, and probable impact on private cloud environment. *Big Data Analytics for Internet of Things*, Wiley Online Library, p. 285–319, 2017. Citado na página 10.

GONDIM, J. J.; ALBUQUERQUE, R. de O.; OROZCO, A. L. S. Mirror saturation in amplified reflection distributed denial of service: A case of study using snmp, ssdp, ntp and dns protocols. *Future Generation Computer Systems*, Elsevier, v. 108, p. 68–81, 2020. Citado 2 vezes nas páginas 4 e 9.

HAQUE, M. R. et al. Unprecedented smart algorithm for uninterrupted sdn services during ddos attack. *Computers, Materials & Continua*, Tech Science Press, v. 70, n. 1, p. 875–894, 2022. Citado na página 8.

HEINRICH, T. Análise longitudinal de dados do dnspot. In: . [S.l.: s.n.], 2017. Citado na página 17.

HEINRICH, T. *Caracterizaçao de Ataques DRDoS Usando Honeypot*. Tese (Doutorado) — Dissertaçao de mestrado em Computaçao Aplicada, UDESC, Joinville (SC), 2019. Citado 4 vezes nas páginas 6, 9, 10 e 12.

HEINRICH, T. Caracterização de ataques drdos usando honeypot. In: . [s.n.], 2019. Disponível em: <https://www.udesc.br/arquivos/cct/id_cpmenu/1024/Disserta___o_completa_15699280495759_1024.pdf>. Citado 6 vezes nas páginas 7, 8, 9, 14, 15 e 17.

HEINRICH, T.; OBELHEIRO, R. R.; MAZIERO, C. A. New kids on the drdos block: Characterizing multiprotocol and carpet bombing attacks. In: SPRINGER. *International Conference on Passive and Active Network Measurement*. [S.l.], 2021. p. 269–283. Citado 3 vezes nas páginas 6, 10 e 11.

HOEPERS, C.; JESSEN, K. S.; CHAVES, M. Honeypots e honeynets: Definições e aplicações. *Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, ver*, 2007. Disponível em: <https://www.cert.br/docs/whitepapers/honeypots-honeynets/#ref-02>. Citado 2 vezes nas páginas 5 e 9.

HOFFMAN, P.; SULLIVAN, A.; FUJIWARA, K. *RFC 8499: DNS Terminology*. [S.l.], 2019. Citado na página 15.

HUBERT, A.; MOOK, R. V. *Measures for making DNS more resilient against forged answers*. [S.l.], 2009. Citado na página 18.

HUSÁK, M.; VIZVÁRY, M. Poster: Reflected attacks abusing honeypots. In: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. [S.l.: s.n.], 2013. p. 1449–1452. Citado 2 vezes nas páginas 5 e 10.

JONKER, M. et al. Millions of targets under attack: a macroscopic characterization of the dos ecosystem. In: *Proceedings of the 2017 Internet Measurement Conference*. [S.l.: s.n.], 2017. p. 100–113. Citado 2 vezes nas páginas 4 e 11.

KHANDELWAL, S. World's largest 1tbps ddos attack launched from 152,000 hacked smart devices. *The Hacker News*, 2016. Citado na página 8.

KRÄMER, L. et al. Amppot: Monitoring and defending against amplification ddos attacks. In: SPRINGER. *International Symposium on Recent Advances in Intrusion Detection*. [S.l.], 2015. p. 615–636. Citado 4 vezes nas páginas 5, 9, 10 e 12.

LEMOS, R. *History Shows DDoS Volumes to Keep Rising Despite Mitigation Efforts*. 2018. <https://www.eweek.com/security/how-ddos-attacks-techniques-have-evolved-over-past-20-years/>. (Accessed on 01/09/2022). Citado na página 8.

LOPES, R. W. *Ataques DDoS Panorama, Mitigação e Evolução*. 2015. <https://ftp.registro.br/pub/gter/gter39/08-AtaquesDdosPanoramaMitigacaoEvolucao.pdf>. (Accessed on 01/09/2022). Citado na página 8.

MOCKAPETRIS, P. *Domain names-concepts and facilities*. [S.l.], 1987. Citado na página 15.

NEWMAN, L. H. Github survived the biggest ddos attack ever recorded. *Wired*, v. 1, 2018. Citado na página 8.

NIST. *NVD - CVE-1999-1379*. 1999. <https://nvd.nist.gov/vuln/detail/CVE-1999-1379>. (Accessed on 01/09/2022). Citado na página 8.

NOROOZIAN, A. et al. Who gets the boot? analyzing victimization by ddos-as-a-service. In: SPRINGER. *International Symposium on Research in Attacks, Intrusions, and Defenses*. [S.l.], 2016. p. 368–389. Citado na página 11.

PARTRIDGE, C. *Mail routing and the domain system*. [S.l.], 1986. Citado na página 15.

PRINCE, M. *The DDoS That Almost Broke the Internet. blog. cloudflare. com/the-ddos-that-almost-broke-the-internet*. [S.l.]: March, 2013. Citado na página 8.

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 8.

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

REED, J. A.; REED, J. Potential email compromise via dangling dns mx. 2020. Citado na página 15.

ROSSOW, C. Amplification hell: Revisiting network protocols for ddos abuse. In: *NDSS*. [S.l.: s.n.], 2014. Citado 5 vezes nas páginas 4, 6, 7, 10 e 11.

RYBA, F. J. et al. Amplification and drdos attack defense–a survey and new perspectives. *arXiv preprint arXiv:1505.07892*, 2015. Citado 2 vezes nas páginas 8 e 10.

THOMAS, D. R.; CLAYTON, R.; BERESFORD, A. R. 1000 days of udp amplification ddos attacks. In: IEEE. *2017 APWG Symposium on electronic crime research (eCrime)*. [S.l.], 2017. p. 79–84. Citado 2 vezes nas páginas 4 e 11.

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

WOODY, C.; MEAD, N.; SHOEMAKER, D. Foundations for software assurance. In: IEEE. *2012 45th Hawaii International Conference on System Sciences*. [S.l.], 2012. p. 5368–5374. Citado na página 8.

XU, R. et al. A drdos detection and defense method based on deep forest in the big data environment. *Symmetry*, Multidisciplinary Digital Publishing Institute, v. 11, n. 1, p. 78, 2019. Citado na página 10.

ZETTER, K. Lazy hacker and little worm set off cyberwar frenzy. *Wired News. http://www. wired. com/threatlevel/2009/07/mydoom*, 2009. Citado na página 8.

ZHAUNIAROVICH, Y.; DODIA, P. Sorting the garbage: filtering out drdos amplification traffic in isp networks. In: IEEE. *2019 IEEE Conference on Network Softwarization (NetSoft)*. [S.l.], 2019. p. 142–150. Citado na página 10.