Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

ANÁLISE DE PADRÕES DE TRÁFEGO DDOS EM DATASETS PÚBLICOS E SUA CORRELAÇÃO COM ARQUITETURAS DE MITIGAÇÃO EM CLOUD COMPUTING

ANALYSIS OF DDOS TRAFFIC PATTERNS IN PUBLIC DATASETS AND THEIR CORRELATION WITH MITIGATION ARCHITECTURES IN CLOUD COMPUTING

João Vitor Lopes Bezerra, Faculdade de Tecnologia de Americana "Ministro Ralph Biasi" joao.bezerra2@fatec.sp.gov.br
Lucas Jacomini Levighin, Faculdade de Tecnologia de Americana "Ministro Ralph Biasi" lucas.levighin@fatec.sp.gov.br
Prof. Ms. Clerivaldo José Roccia, Faculdade de Tecnologia de Americana "Ministro Ralph Biasi" clerivaldo.roccia@fatec.sp.gov.br

Resumo

Ataques de Negação de Serviço Distribuído (DDoS) hipervolumétricos e multi-vetoriais representam uma ameaça crítica à disponibilidade de serviços em *Cloud Computing*. Este trabalho investiga a eficácia da arquitetura de mitigação integrada em *Cloud Computing* contra ataques de Negação de Serviço Distribuído (DDoS) hipervolumétricos e multi-vetoriais. A metodologia empregou uma abordagem híbrida, combinando a revisão das técnicas de defesa em nuvem (*Anycast*, BGP *FlowSpec*, *Machine Learning*) com a análise quantitativa de *datasets* de tráfego de rede (legítimo vs. malicioso) obtidos no Kaggle. A análise revelou assinaturas comportamentais claras dos ataques, como picos de Pacotes por Segundo (pps) e fluxos de curta duração, validando a necessidade da inteligência comportamental para complementação das defesas de escala distribuída. Conclui-se que a resiliência contra as ameaças modernas exige, necessariamente, a integração de múltiplas camadas de segurança baseadas em nuvem.

Palavras-chave: Ataque DDoS, Cloud Computing, Botnet, Defesa em Nuvem, Ataque Hipervolumétrico.

Abstract

Hypervolumetric and multi-vector Distributed Denial of Service (DDoS) attacks pose a critical threat to the availability of services in Cloud Computing. This study investigates the effectiveness of integrated mitigation architecture in Cloud Computing against hypervolumetric and multi-vector Distributed Denial of Service (DDoS) attacks. The methodology employed a hybrid approach, combining a review of cloud defense techniques (Anycast, BGP FlowSpec, Machine Learning) with a quantitative analysis of network traffic datasets (legitimate vs. malicious) obtained from Kaggle. The analysis revealed clear behavioral attack signatures, such as high Packets-Per-Second (pps) peaks and short-duration flows, validating the necessity of behavioral intelligence to complement distributed scale defenses. It is concluded that resilience against modern threats necessarily requires the integration of multiple cloud-based

security layers.

***Keywords**: DDoS Attack, Cloud Computing, Botnet, Cloud Defense, Hypervolumetric Attack.*

1. Introdução

Com a crescente digitalização de serviços e a dependência de sistemas baseados em nuvem, a disponibilidade de recursos online tornou-se uma prioridade crítica para organizações em todo o mundo. Os ataques de *Distributed Denial Of Service* (DDoS) permanecem como um sério risco à continuidade operacional de serviços essenciais da Internet, aplicações web e ambientes em nuvem. Apesar dos inúmeros estudos voltados à identificação e mitigação desse tipo de ameaça, sua eliminação definitiva ainda não foi alcançada. Além disso, as técnicas utilizadas nesses ataques seguem em constante transformação, exigindo análises atualizadas e alinhadas à realidade atual do cenário de ameaças (Hohlfeld, Dietzel, Kopp, 2021).

Com o passar do tempo, os ataques de natureza volumétrica têm se tornado mais frequentes e sofisticados. A constante capacidade dos agentes maliciosos de ajustarem suas estratégias frente às soluções de defesa existentes torna essencial que o setor mantenha um monitoramento contínuo e uma análise aprofundada dos ataques em curso (Boin *et al*., 2022).

Diante disso, este estudo tem como problema de pesquisa identificar como a integração de tecnologias de *Cloud Computing* pode mitigar de forma eficaz os ataques DDoS hipervolumétricos e multi-vetoriais, garantindo a continuidade e a disponibilidade dos serviços críticos na Internet. Para tanto, busca como objetivo geral analisar a arquitetura de mitigação integrada em *Cloud Computing*, detalhando como a combinação de escala distribuída, filtragem de borda e inteligência comportamental oferece resiliência superior contra a crescente sofisticação e volume (Tbps) dos ataques DDoS modernos. Como objetivos específicos, realizar um levantamento da literatura das técnicas de mitigação em *Cloud Computing*, com foco em arquiteturas *Anycast*, BGP *FlowSpec* e *Machine Learning*, analisar e comparar conjuntos de dados públicos de tráfego de rede (obtidos via Kaggle), a

fim de identificar as assinaturas comportamentais e os diferenciais de volume entre o tráfego de rede legítimo e o tráfego de ataques DDoS que validam a necessidade de mecanismos de *Machine Learning* como estrategia de mitigação e por fim, justificar a aplicação das tecnologias de defesa em nuvem (*Anycast,* BGP *FlowSpec* e *Machine Learning*) e correlacionar sua eficácia com os padrões de ataque identificados, validando a abordagem de mitigação em múltiplas camadas.

2. Referencial Teórico

O presente Referencial Teórico é estruturado para fornecer a fundamentação bibliográfica e técnica indispensável à análise proposta neste trabalho. Inicialmente, são apresentados os conceitos de *Cloud Computing* e a arquitetura de redes envolvida, seguidos por uma discussão sobre a evolução das ameaças DDoS, a ascensão da IoT como vetor de ataque. A seção finaliza com o detalhamento das principais tecnologias de mitigação em nuvem: *Anycast*, BGP *FlowSpec* e *Machine Learning*, cujo embasamento teórico permitirá a correlação com os padrões de ataque identificados, validando a arquitetura de defesa em múltiplas camadas.

2.1 Segurança da Informação

A segurança da informação refere-se à proteção dos dados contra acessos não autorizados, alterações indevidas e destruição acidental ou intencional. Segundo Stallings (2017), ela abrange um conjunto de políticas, procedimentos e ferramentas projetadas para assegurar a proteção dos ativos informacionais. Ataques a sistemas computacionais ocorrem, geralmente, pela exploração de vulnerabilidades, que podem ser técnicas, humanas ou procedimentais. "A segurança da informação existe para proteger dados contra ameaças internas e externas, garantindo que os mesmos estejam acessíveis apenas a quem for autorizado" (Stallings, 2017, p. 5).

De acordo com Pfleeger, Pfleeger e Margulies (2015), uma vulnerabilidade é uma fraqueza que pode ser explorada por uma ameaça para violar a segurança de um sistema. Os ataques ocorrem motivados por interesses financeiros, políticos, ideológicos ou apenas pelo desafio técnico. Muitas vezes, os invasores se aproveitam da ausência de atualizações, da má configuração de serviços ou da falta de conscientização dos usuários.

2.2 Importância da Segurança da Informação

Com o avanço contínuo da transformação digital, as organizações enfrentam um cenário de crescente exposição a riscos cibernéticos. A dependência de sistemas informatizados para a realização de operações críticas exige a adoção de práticas robustas de segurança da informação, capazes de garantir a resiliência dos serviços diante de ameaças internas e externas (Whitman; Mattord, 2018).

Além disso, a segurança da informação tem se tornado um pilar estratégico, não apenas para proteção de ativos, mas também para a manutenção da confiança de clientes e parceiros. A ausência de controles eficazes pode resultar em impactos financeiros, danos à reputação e comprometimento da continuidade de negócios (ISO, 2013). Em um contexto no qual vazamento de dados, ataques de *ransomware* e negações de serviços, são cada vez mais frequentes, a implementação de políticas e medidas de proteção, torna-se essencial para garantir a disponibilidade, integridade e confidencialidade das informações (Pfleeger, Pfleeger, Margulies, 2015).

2.3 Pilares da Segurança da Informação

A Segurança da Informação é regida por pilares essenciais: **Confidencialidade** (proteção contra acesso indevido), **Integridade** (garantia da precisão e completude dos dados) e **Disponibilidade** (acessibilidade e usabilidade da informação quando necessária) (Whitman e Mattord, 2018, p. 36; Tipton e Krause, 2008). Dentre estes, a **Disponibilidade** é o foco principal de ataques como o DDoS, que visam tornar os recursos de rede inoperantes e

interromper o acesso a serviços críticos, conforme assegura a ABNT NBR ISO/IEC 27002 (2013) e é detalhado por Mirkovic e Reiher (2004).

2.4 Ataque DDoS

Um ataque de negação de serviço distribuído (DDoS) consiste em sobrecarregar servidores, redes ou serviços com tráfego malicioso, tornando-os indisponíveis para usuários legítimos. Segundo a Cloudflare (2025c), esses ataques interrompem o tráfego normal ao inundar a infraestrutura com um volume massivo de dados, causando prejuízos financeiros, danos à reputação e perda de confiança dos clientes. Os ataques DDoS evoluíram a partir dos ataques DoS, impulsionados pela expansão da internet. O primeiro ataque DDoS documentado ocorreu em 1999, com a ferramenta Trinoo usada para atacar a Universidade de Minnesota, derrubando seus serviços por mais de dois dias (Radware, 2017). Conforme Mirkovic e Reiher (2004), os DDoS deixaram de ser apenas ataques de inundação, passando a explorar falhas em protocolos e aplicações. Em 2000, o hacker "Mafiaboy" realizou uma série de ataques contra grandes empresas como Yahoo! e Amazon, demonstrando o potencial destrutivo dessas ofensivas.

Com o tempo, os ataques tornaram-se mais frequentes e sofisticados, baseando-se em *botnets*, redes de dispositivos comprometidos controladas remotamente para ampliar seu impacto (Zhang, Wang; Fu, 2024). Além de interromper serviços, essas ações causam perdas diretas e indiretas, podendo ainda servir como distração para invasões e exfiltração de dados sensíveis (Whitman; Mattord, 2017).

Mirkovic e Reiher (2004) explicam que os DDoS podem ser classificados conforme a camada alvo, o tipo de tráfego e o método de ataque. Relatório da Cloudflare mostra que, em 2024, foram bloqueados 21,3 milhões de ataques, um aumento de 53% em relação a 2023, com média de 4.870 bloqueios por hora. Destacam-se os ataques hipervolumétricos, com mais de 1 bilhão de pacotes por segundo ou 1 Tbps. Somente no último trimestre referente ao ano de 2024, mais de 420 ataques superaram 1 Tbps, com crescimento de 1.885% em relação ao trimestre

anterior. Durante o Halloween, de 2024, a Cloudflare neutralizou o maior ataque já registrado: 5,6 Tbps (Cloudflare, 2024).

Esses números evidenciam a crescente potência dos DDoS e reforçam a necessidade urgente de soluções de defesa robustas, especialmente em ambientes de computação em nuvem, onde a disponibilidade é crítica para a continuidade dos negócios.

2.5 Botnets

Nas últimas décadas, o avanço das tecnologias de comunicação e a massiva conectividade digital transformaram a forma como dispositivos interagem na internet, mas também ampliaram significativamente a superfície de ataque para cibercriminosos. Nesse cenário, uma das ameaças mais recorrentes e perigosas é o uso de redes coordenadas de dispositivos comprometidos, conhecidas como *botnets*. O termo *botnet* é uma junção de "*robot*" e "*network*" — uma rede de computadores zumbis controlados remotamente por um agente malicioso, conhecido como *botmaster* ou *herder*. Esses dispositivos comprometidos, também chamados de bots ou zumbis, podem ser computadores pessoais, servidores e até dispositivos IoT, que após infectados por malwares passam a atender comandos remotos de forma silenciosa e automatizada (Cloudflare, 2023a).

As *botnets* são essenciais para a realização de ataques DDoS, pois permitem ao atacante coordenar um grande volume de requisições simultâneas a um alvo específico, excedendo sua capacidade de resposta e, assim, causando interrupções. A eficiência desses ataques está diretamente relacionada ao tamanho da *botnet* e à diversidade geográfica de seus dispositivos infectados, dificultando a mitigação pela dispersão dos vetores (Mirkovic; Reiher, 2004). A formação de uma *botnet* geralmente se inicia com a disseminação de um malware que explora vulnerabilidades conhecidas em sistemas operacionais ou aplicativos, permitindo a instalação de *backdoors*. Esses *malwares* são distribuídos por meio de campanhas de *phishing*, *downloads* maliciosos ou exploração de dispositivos mal configurados. Uma vez comprometido, o dispositivo se conecta a um servidor de comando e controle (C&C), de onde passa a receber

instruções do operador da *botnet* (Cloudflare, 2023a).

Dentre as *botnets* mais notórias da história, destaca-se a Mirai, que em 2016 se popularizou por infectar dispositivos IoT (*Internet of Things*) vulneráveis, como câmeras IP, roteadores domésticos e gravadores de vídeo digital — utilizando credenciais padrão fracas. A *botnet* Mirai foi responsável por um ataque DDoS massivo contra o provedor Dyn, o qual afetou grandes serviços da internet como Twitter, Netflix e GitHub (Antonakakis *et al.*, 2017). Segundo Antonakakis *et al.* (2017), o sucesso da Mirai evidenciou o papel crítico dos dispositivos IoT na amplificação de ataques DDoS, devido à sua ampla distribuição, falta de atualizações de segurança e configurações padrão expostas. Essa nova classe de dispositivos ampliou consideravelmente a superfície de ataque, gerando *botnets* com milhões de nós.

Como aponta a Cloudflare (2023b), *botnets* modernas têm adotado técnicas sofisticadas para evitar detecção e bloqueio. Entre elas está a utilização de arquiteturas descentralizadas baseadas em redes *peer-to-peer* (P2P), que eliminam a dependência de um servidor de comando e controle centralizado. Nessa abordagem, cada dispositivo comprometido (*bot*) é capaz de se comunicar diretamente com outros *bots* da rede, o que torna a estrutura mais resiliente: mesmo que parte da rede seja desativada, os *bots* restantes continuam operando e trocando comandos. Além disso, essas redes maliciosas frequentemente utilizam canais de comunicação criptografados, dificultando a interceptação e análise do tráfego. Outra técnica comum é o uso de domínios de curta duração, por meio de algoritmos de geração de domínios (*domain flux*), o que complica ações de bloqueio e derrubada de servidores C&C por parte das autoridades ou provedores de serviço. Com o avanço da computação em nuvem, as *botnets* também passaram a explorar infraestruturas *cloud* comprometidas, alocando recursos temporários para lançar ataques com alta capacidade de banda. A Cloudflare observou, por exemplo, que *botnets* modernas como a Mantis foram capazes de atingir picos superiores a 71 milhões de requisições por segundo (rps), utilizando menos de 5.000 *bots*, o que mostra o potencial destrutivo mesmo com uma rede reduzida (Cloudflare, 2023c).

A relevância das *botnets* nos ataques DDoS não reside apenas na quantidade de máquinas envolvidas, mas na capacidade de automação e evasão que oferecem aos atacantes.

Segundo Mirkovic e Reiher (2004), os ataques DDoS mais bem-sucedidos são aqueles conduzidos por *botnets* distribuídas geograficamente e com múltiplos vetores de ataque simultâneos, como UDP *floods*, TCP SYN *floods* e HTTP *floods*.

Além do impacto técnico, *botnets* representam um problema jurídico e forense (aplicação de métodos e técnicas para a investigação e elucidação de crimes ou incidentes) considerável. Como a origem dos ataques é mascarada pelo uso de dispositivos de terceiros, muitas vezes em diferentes países, a investigação torna-se complexa e exige cooperação internacional, algo que ainda representa um grande desafio para autoridades (Whitman; Mattord, 2017).

2.5.1 Influência de dispositivos IoT em *botnets*

O avanço da conectividade digital impulsionou a ascensão da Internet das Coisas (IoT), caracterizada pela rede de dispositivos físicos integrados que coletam e compartilham dados sem intervenção humana (Fernandes; Jung; Prakash, 2017, p. 636–654). Esse crescimento é exponencial, com a Statista (2024) estimando um salto de 17,1 bilhões de dispositivos conectados em 2024 para 29 bilhões até 2030. Contudo, a rápida adoção da IoT não foi acompanhada por práticas de segurança robustas. Muitos dispositivos são vulneráveis (senhas fracas, falta de atualização), tornando-se alvos fáceis para agentes maliciosos e o recrutamento em *botnets* (Kolias et al., 2017).

Neste cenário de vulnerabilidade expandida, a IoT se estabeleceu como o vetor principal por trás dos ataques de negação de serviço distribuída (DDoS) de maior magnitude. A força de uma *botnet* baseada em IoT reside na sua distribuição geográfica e no alto número de nós controlados, o que expandiu a superfície de ataque e tornou as *botnets* mais resilientes (Kolias et al., 2017). Como exemplo da dimensão dessa ameaça, a Cloudflare (The Hacker News, 2025)

mitigou em 2024 um ataque DDoS recorde de 5,6 terabits por segundo (Tbps), impulsionado por uma variante da notória *botnet* Mirai e composto por mais de 13.000 dispositivos IoT comprometidos. Portanto, a ascensão da IoT representa um vetor crescente de risco, justificando a necessidade urgente de defesas escaláveis e distribuídas.

2.6 Computação em Nuvem

Nas últimas décadas, a evolução tecnológica transformou o acesso, o processamento e o armazenamento de dados, consolidando a Computação em Nuvem (*Cloud Computing*) como um marco significativo. Este modelo rompe com a lógica de infraestrutura local ao entregar recursos computacionais (servidores, armazenamento, aplicações) como serviços remotos e sob demanda, via Internet (Akamai, 2025a). A CC estabeleceu-se como uma peça-chave na transformação digital, provendo a flexibilidade, a economia de custos e, crucialmente, a escalabilidade necessária para ambientes dinâmicos e de alta demanda. A Akamai Technologies (2025a) define-a como "o fornecimento de serviços de computação... por meio da Internet ('a nuvem') com pagamento conforme o uso", eliminando a necessidade de infraestrutura física local e oferecendo a agilidade requerida para enfrentar demandas variadas.

2.6.1 Origem da Computação em Nuvem

A origem da computação em nuvem remonta à visão de John McCarthy na década de 1960, que preconizou a organização da computação como um serviço público (*utility computing*) acessível sob demanda (TDSynnex, 2020). Embora o conceito tenha evoluído nas décadas seguintes com o avanço da virtualização e das redes, o marco comercial mais significativo ocorreu em 2006, com o lançamento da Amazon Web Services (AWS). A AWS, por meio de serviços como o Elastic Compute Cloud (EC2), permitiu o aluguel flexível e escalável de poder de processamento (AWS, 2025). Esse movimento transformou o consumo de TI, substituindo altos investimentos em *data centers* próprios por custos operacionais

proporcionais ao uso, estabelecendo o paradigma moderno da nuvem.

2.6.2 Importância e os benefícios da cloud computing atualmente

A Computação em Nuvem transformou o acesso a recursos de TI, tornando-se essencial na transformação digital. Sua principal vantagem reside na escalabilidade sob demanda, que permite o ajuste dinâmico de recursos para lidar com variações extremas de carga (Akamai, 2025a). Essa característica, aliada à alta disponibilidade provida por *data centers* distribuídos globalmente, garante redundância e continuidade de serviços, sendo crucial no combate a ataques hipervolumétricos. Adicionalmente, o modelo de pagamento por uso e a eliminação da necessidade de infraestrutura física local oferecem economia de custos. A nuvem também sustenta tecnologias emergentes como *Machine Learning* e *Big Data*, as quais são vitais para o desenvolvimento de algoritmos que aprendem padrões anômalos, reforçando a inteligência na segurança cibernética (Microsoft, 2025)

2.6.3 Modelos de implantação em *Cloud Computing*

A implantação em nuvem é estratégica e baseia-se em três modelos principais (Intel, 2025). A Nuvem Pública utiliza infraestrutura gerenciada por terceiros e compartilhada, oferecendo máxima escalabilidade sob demanda e o modelo de pagamento por uso. A Nuvem Privada é exclusiva a uma única organização, priorizando controle, segurança e conformidade, sendo hospedada localmente ou por provedores. Por fim, a Nuvem Híbrida combina os ambientes público e privado, permitindo a movimentação de dados e aplicações para otimizar recursos, flexibilidade e desempenho em cenários com demandas variáveis ou exigências regulatórias (Microsoft, 2025). Essa diversidade de modelos influencia diretamente as estratégias de resiliência digital adotadas pelas empresas.

2.6.4 Modelos de serviços em *Cloud Computing*

Os modelos de serviço representam formas distintas de entrega de recursos tecnológicos, que definem os níveis de gerenciamento e responsabilidade entre o provedor e o cliente (Microsoft, 2025). Três modelos se consolidaram como pilares desse ecossistema, assim definidas pela empresa: Infraestrutura como Serviço (IaaS), que fornece recursos fundamentais (máquinas virtuais, redes e armazenamento) para que os usuários gerenciem sua própria infraestrutura; Plataforma como Serviço (PaaS), que oferece um ambiente completo para desenvolvimento e implantação de aplicações, com toda a infraestrutura subjacente gerenciada pelo provedor; e Software como Serviço (SaaS), que disponibiliza softwares completos e prontos para uso, nos quais todo o gerenciamento é de responsabilidade do provedor.

2.7 Segurança em *Cloud Computing*

A segurança na computação em nuvem é uma preocupação central, visto que o modelo centraliza dados e serviços sensíveis em uma infraestrutura distribuída globalmente (Akamai, 2025b). Provedores como AWS, Azure e Google Cloud operam data centers que, embora ampliem a eficiência e a escalabilidade, também aumentam a superfície de exposição a ameaças. A arquitetura *multitenant* exige a aplicação de controles rigorosos de acesso, monitoramento contínuo e estrita conformidade com normas internacionais como ISO/IEC 27017 e NIST SP 800-144 (IBM, 2025).

Neste contexto, o ataque DDoS é um risco proeminente, pois visa a indisponibilidade de serviços ao sobrecarregar recursos computacionais ou de rede. Em ambientes de nuvem, sua propagação é potencializada pela alta largura de banda e elasticidade dos sistemas, podendo afetar serviços interligados e gerar grandes prejuízos (Akamai, 2025b). Os ataques são classificados em vetores volumétricos (saturação de banda, ex: UDP *flood*), de protocolo (exploração de falhas em camadas L3/L4, ex: SYN *flood*) ou de aplicação (sobrecarga de software, ex: HTTP *flood*). A gravidade desses eventos é comprovada pelos recordes recentes de mitigação: 2,3 Tbps pela AWS em 2020, 3,47 Tbps pela Microsoft em 2021 e o registro de

46 milhões de requisições por segundo pela Google Cloud em 2022. Esses casos demonstram a capacidade destrutiva das *botnets* e sublinham o desafio contínuo de proteger a nuvem contra ameaças massivas e multi-vetoriais (Cloudflare, 2025b).

2.8 As principais técnicas de mitigação (Anycast, BGP FlowSpec, Machine Learning)

A mitigação de ataques DDoS em ambientes de computação em nuvem representa uma das frentes mais sofisticadas da segurança cibernética moderna, exigindo soluções que operem em tempo real, com capacidade de escalar horizontalmente diante de tráfegos maliciosos massivos. Esses ataques, como já explanado anteriormente, visam exaurir os recursos computacionais de uma infraestrutura ou derrubar sua disponibilidade, por meio da sobrecarga de tráfego gerado por redes distribuídas de dispositivos comprometidos, conhecidas como *botnets*. Cada vetor de ataque possui suas características técnicas específicas, como o HTTP *flood*, que simula requisições legítimas de páginas web com altíssima frequência para exaurir o pool de threads de servidores web; o SYN flood, que abusa do processo de *handshake* do protocolo TCP, enviando pacotes SYN sem completar a conexão, mantendo recursos ocupados indefinidamente; o ACK *flood*, que sobrecarrega servidores com pacotes TCP ACK em alta taxa, explorando o estado da conexão; o UDP *flood*, que envia grandes volumes de pacotes UDP a portas aleatórias; e o ICMP *flood*, que abusa do protocolo de mensagens de controle da Internet com pacotes tipo "*ping*" (Cloudflare, 2025c; Cloudflare, 2025d; Cloudflare, 2025e; Cloudflare, 2025f). O avanço dos ataques DDoS, especialmente aqueles que superam múltiplos terabits por segundo, como o ataque de 3,8 Tbps mitigado pela Cloudflare em 2023 (Cloudflare, 2025g), torna essencial a integração de sistemas autônomos altamente distribuídos.

A mitigação moderna é estruturada em torno de duas tecnologias cruciais: a escala e a inteligência. A escala é alcançada por meio de Redes de Distribuição de Conteúdo (CDNs) que operam em arquitetura *Anycast*. Essa arquitetura absorve e fragmenta o tráfego em múltiplos datacenters que compartilham o mesmo IP, roteando-o para o nó geograficamente mais

próximo, o que aumenta a resiliência e a latência (Cloudflare, 2025h). Complementarmente, provedores de nuvem empregam o protocolo BGP (*Border Gateway Protocol*) com a extensão BGP *FlowSpec* para distribuir regras de filtragem em tempo real, mitigando ataques volumétricos diretamente nos pontos de entrada da rede (Sage Networks, 2024; Cloudflare, 2025i).

A inteligência é garantida pela automação e *Machine Learning*. Plataformas modernas utilizam sistemas de detecção que analisam padrões de tráfego (como taxa de pacotes e *headers* HTTP) para acionar defesas dinâmicas contra vetores de Aplicação. Provedores como Google Cloud, AWS e Microsoft Azure oferecem serviços nativos de proteção DDoS (Azure DDoS Protection, AWS Shield), que atuam de forma transparente e escalável, reforçando a defesa. A eficiência final destas soluções é potencializada pela cooperação e inteligência compartilhada entre todo o ecossistema (ISPs, IXPs e fornecedores de segurança), garantindo a continuidade dos serviços críticos sob cenários extremos (Akamai, 2025c; Cloudflare, 2025j).

3. Materiais e Métodos

O presente trabalho emprega uma abordagem metodológica híbrida, combinando a revisão da literatura para a fundamentação teórica com a pesquisa quantitativa xxploratória para a análise prática, visando validar as estratégias de mitigação em *Cloud Computing*.

3.1 Tipo e procedimento de pesquisa

A pesquisa foi estruturada em duas etapas principais: Fundamentação Teórica (revisão da literatura): foi realizado um levantamento sistemático de fontes teóricas, incluindo artigos científicos, *white papers* de segurança (como Cloudflare) e publicações especializadas. O foco foi a arquitetura e as técnicas de mitigação (*Anycast*, WAF, BGP *FlowSpec*) aplicadas ao contexto de ataques DDoS hipervolumétricos.

Análise de Dados (Pesquisa Quantitativa): Nesta fase, procedeu-se à análise

comparativa de conjuntos de dados (*datasets*) públicos obtidos na plataforma Kaggle. A amostra utilizada consistiu em uma amostragem de milhares de registros de fluxos de rede, categorizados em Tráfego Malicioso (ataques DDoS) e Tráfego Legítimo (uso normal).

3.2. Instrumento e Foco da Análise

O instrumento de análise consistiu na criação de seis visualizações estatísticas e gráficos comparativos. O processamento dos dados teve como objetivo isolar as assinaturas do tráfego de ataque, concentrando-se nas seguintes métricas-chave:

- Volume: Diferencial de taxa de Pacotes por Segundo (pps).
- Vetor: Prevalência de Protocolos (UDP/TCP) e Portas (80/443).
- Comportamento: Distribuição da Duração dos Fluxos e Tamanho dos Pacotes.

O produto final desta metodologia é a discussão dos resultados, que utiliza os gráficos gerados como prova empírica para correlacionar a ameaça com a necessidade das soluções de segurança baseadas em *Cloud Computing*.

4. Resultados e Discussões

As análises comparativas entre tráfego benigno e malicioso foram realizadas a partir de conjuntos de dados públicos de detecção de intrusão (IDS) amplamente reconhecidos na área de segurança, como CSE-CIC-IDS2018-AWS, CICIDS2017 e CIC DoS Dataset de 2016. Esses *datasets* contêm fluxos de rede legítimos e de ataques DDoS, que foram extraídos e combinados para formar conjuntos balanceados e desbalanceados. O primeiro conjunto, final_dataset.csv, possui cerca de 12,7 milhões de registros e 84 características, enquanto o segundo, unbalanced_20_80_dataset.csv, contém aproximadamente 7,6 milhões de registros, com 20% de tráfego DDoS e 80% benigno.

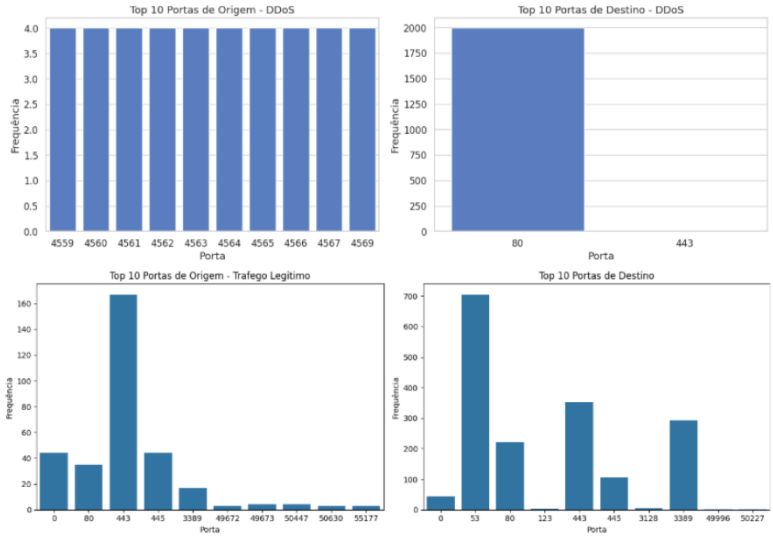
Devido ao grande volume de dados, utilizou-se uma amostragem de 2000 linhas de cada conjunto, preservando a representatividade estatística, assim formando o primeiro e o segundo experimento. As análises foram conduzidas com base nas colunas Protocol, Src Port, Dst Port, Src IP, Dst IP, Pkt Len Mean, Flow Pkts/s e Flow Duration, utilizando o Google Colab como ambiente laboratorial utilizando linguagem Python em conjunto com a biblioteca Pandas para gerar os gráficos, permitindo comparar o comportamento das métricas entre os fluxos benignos e os de ataque. Essas variáveis possibilitaram observar diferenças significativas na distribuição de portas, IPs, protocolos e padrões de pacotes, evidenciando características típicas de tráfego DDoS.

Foi desenvolvido um terceiro experimento com cerca de 800 mil registros de tráfego misto (DDoS e benigno), analisando as variáveis *Packet Length, Packets/Time e Transport Layer*. Essa análise permitiu identificar correlações entre tamanho dos pacotes, taxa de transmissão e protocolos utilizados. Observou-se que o tráfego DDoS apresenta altas taxas de pacotes por segundo, pacotes menores e repetição de endereços e portas, enquanto o tráfego legítimo mostra maior diversidade e duração nos fluxos. Mesmo sem o uso de técnicas de aprendizado de máquina, foi possível distinguir visualmente comportamentos anômalos característicos de ataques DDoS.

Na análise das portas de origem e destino (Figura 1), observam-se diferenças claras entre o tráfego benigno e o associado a ataques DDoS. No cenário de ataque, as portas de origem variam de 4559 a 4569, todas com a mesma frequência, indicando o uso de portas efêmeras para mascarar a origem dos pacotes, comportamento típico de ataques realizados por botnets. Já as portas de destino concentram-se quase exclusivamente nas 80 (HTTP) e 443 (HTTPS), evidenciando um ataque voltado a serviços *web*, com o intuito de sobrecarregar servidores por meio de requisições massivas. De maneira contraria, o tráfego benigno apresenta uma distribuição mais heterogênea de portas, tanto na origem quanto no

destino, com destaque para as portas 443, 445, 80, 53 e 3389, associadas a serviços comuns de rede. Essa variedade reflete a comunicação legítima entre diferentes aplicações, sem concentração em uma única porta, o que caracteriza um comportamento natural e não automatizado de rede.

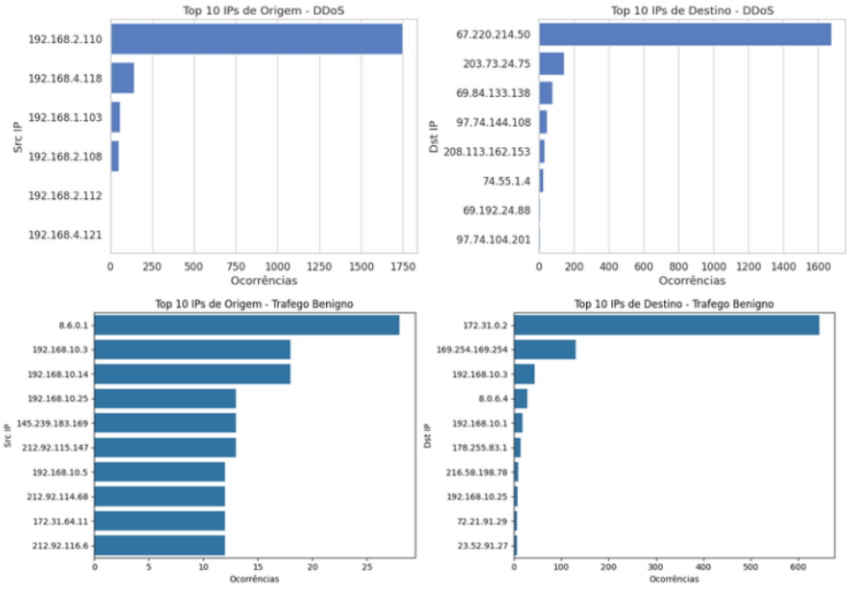
Figura 1 - Comparação de portas origem x destino



Fonte: Próprios Autores

Nos ataques DDoS, observa-se alta concentração de ocorrências em poucos IPs, tanto de origem quanto de destino (Figura 2). O IP de origem 192.168.2.110 domina expressivamente o tráfego, indicando atividade automatizada e centralizada, típica de ataques simulados ou controlados por *botnets*. Da mesma forma, o IP de destino 67.220.214.50 concentra a maior parte dos pacotes, refletindo um ataque direcionado a um único alvo. Em contraste, o tráfego benigno apresenta maior diversidade de endereços IP. As conexões de origem e destino estão distribuídas entre múltiplos endereços, com frequências mais equilibradas, o que é característico de comunicações legítimas em ambientes distribuídos. Essa variação demonstra interações normais entre diferentes *hosts* e serviços.

Figura 2 - Comparação de IPs de origem e destino

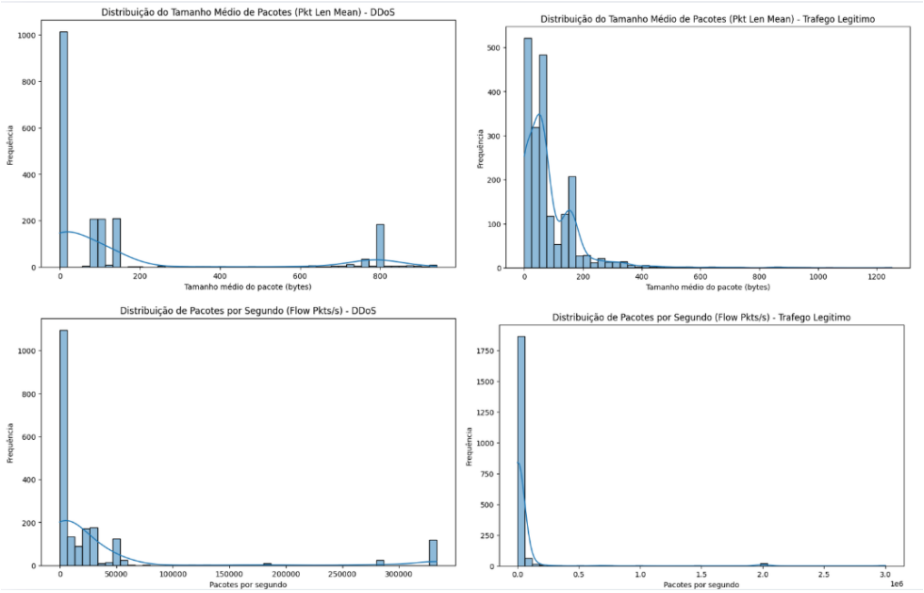


Fonte: Próprios autores

Nos cenários de DDoS, observa-se alta concentração de pacotes com tamanho reduzido e elevada taxa de transmissão, *packets* por segundo (Figura 3). Essa distribuição indica o envio massivo e contínuo de pequenos pacotes, típico de ataques hipervolumétricos que buscam saturar recursos de rede e servidores com grande quantidade de requisições em curto intervalo de tempo.

Já o tráfego legítimo (Figura 3) apresenta maior variabilidade no tamanho dos pacotes e taxas de transmissão mais estáveis, refletindo comunicações reais entre aplicações, com trocas de dados proporcionais à necessidade do serviço. Esse comportamento evidencia fluxos de rede mais equilibrados e duradouros, sem picos abruptos de volume. Sintetizando, o tráfego DDoS caracteriza-se por alta frequência e baixa entropia nos pacotes, enquanto o tráfego benigno demonstra maior diversidade e regularidade, confirmando que métricas como tamanho médio dos pacotes e pacotes por segundo são indicadores eficazes na identificação de comportamentos anômalos em ambientes de *Cloud Computing*.

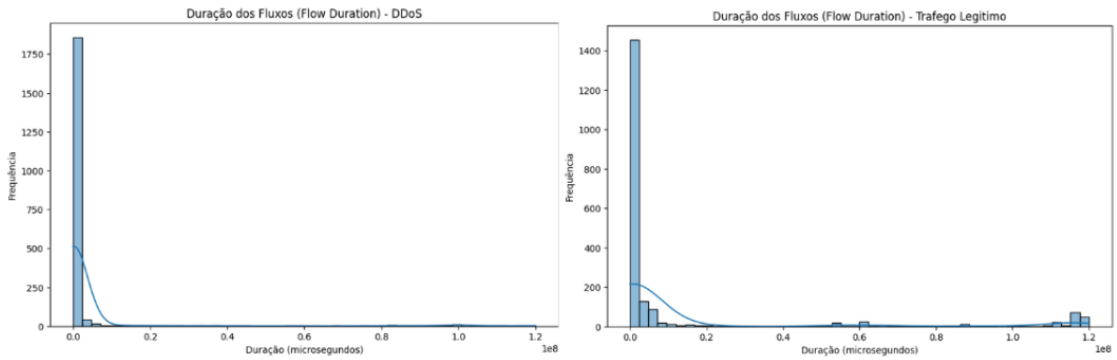
Figura 3 - Comparação de tamanho médio de pacotes e distribuição de pacotes por segundo.



Fonte: Próprios Autores

A análise da duração dos fluxos (Figura 4) evidencia diferenças marcantes entre o tráfego DDoS e o tráfego legítimo. No cenário de ataque DDoS, observa-se uma alta concentração de fluxos de curta duração, com picos próximos a zero microsegundos. Esse comportamento indica conexões efêmeras e repetitivas, resultantes do envio contínuo de pacotes em massa, típicos de ataques automatizados que visam sobrecarregar os recursos de rede sem manter sessões ativas por longos períodos. Ao contrário, o tráfego legítimo apresenta maior variação na duração dos fluxos, incluindo comunicações que se estendem por períodos mais longos. Esse padrão reflete interações reais entre clientes e servidores, nas quais há troca efetiva de dados e manutenção de conexões estáveis.

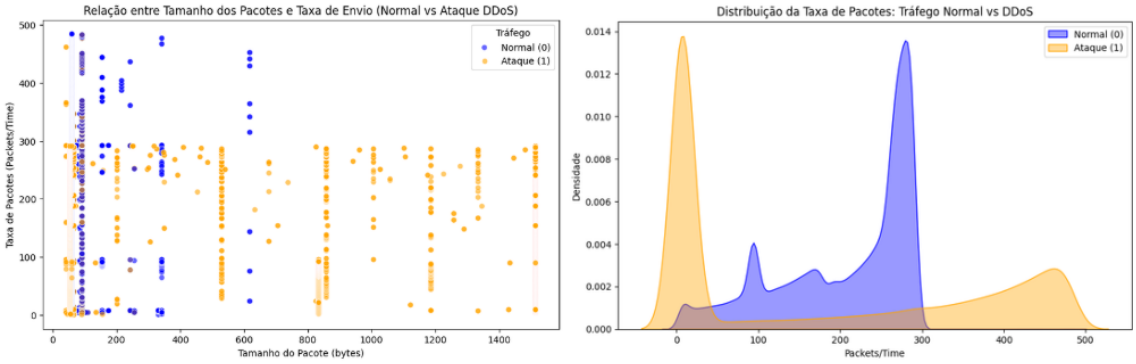
Figura 4 - Comparação de duração dos Fluxos.



Fonte: Próprios Autores

Os gráficos do cenário misto (Figura 5), ilustram a relação entre o tamanho dos pacotes e a taxa de envio (*Packets/Time*), bem como a distribuição da taxa de pacotes para fluxos legítimos e DDoS em um mesmo *dataset*. No primeiro gráfico, observa-se que o tráfego DDoS (em laranja) concentra-se em taxas elevadas de envio, com pacotes de tamanhos variados, enquanto o tráfego normal (em azul) apresenta menores taxas de transmissão e uma distribuição mais coesa de tamanhos de pacotes. Essa diferença evidencia que os ataques DDoS operam com alta frequência de pacotes e baixa regularidade, buscando maximizar o volume de requisições por segundo, um comportamento típico de ataques hipervolumétricos. O segundo gráfico reforça essa distinção: o tráfego benigno apresenta pico acentuado em baixas taxas de pacotes, indicando transmissões regulares e controladas, enquanto o tráfego de ataque mantém valores mais dispersos e com múltiplos picos, representando oscilações abruptas na taxa de envio. Em conjunto, os gráficos demonstram que, mesmo em ambientes de tráfego misto, as métricas de taxa de pacotes e tamanho de pacotes permitem identificar visualmente padrões anômalos associados a ataques DDoS, sem a necessidade de algoritmos complexos. Essa observação reforça a eficácia da análise comportamental como abordagem preliminar para detecção de anomalias em ambientes de *Cloud Computing*.

Figura 5 - Comparação entre relação de tamanho de pacotes e taxa de envio.

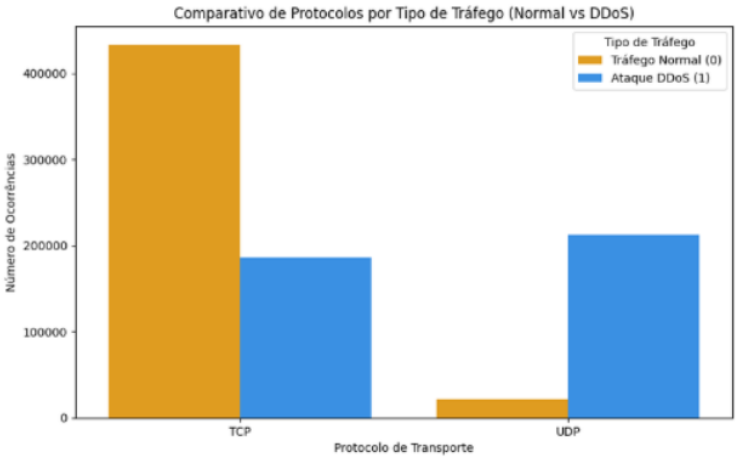


Fonte: Próprios Autores

O seguinte gráfico (Figura 6) compara a utilização dos protocolos TCP e UDP entre o tráfego normal e o tráfego DDoS. Observa-se que o tráfego legítimo é majoritariamente composto por TCP, com número expressivamente superior de ocorrências, o que é esperado em comunicações autênticas de aplicações *web* e serviços corporativos, pois o TCP garante confiabilidade e controle de fluxo.

Já no tráfego de ataque, há aumento considerável no uso de UDP, enquanto o volume de TCP é reduzido em relação ao tráfego normal. Essa predominância de UDP está associada a ataques hipervolumétricos, que exploram a ausência de controle de sessão e de verificação de entrega desse protocolo para gerar grandes volumes de pacotes com baixa sobrecarga de processamento. Dessa forma, o gráfico evidencia que ataques DDoS tendem a explorar o UDP pela sua natureza não orientada à conexão, enquanto o tráfego legítimo mantém o padrão TCP, voltado à confiabilidade. Essa diferença reforça a utilidade da análise de protocolos de transporte como métrica discriminatória na identificação de tráfego anômalo em ambientes de *Cloud Computing*.

Figura 6 - Comparativo de protocolos



Fonte: Próprios autores

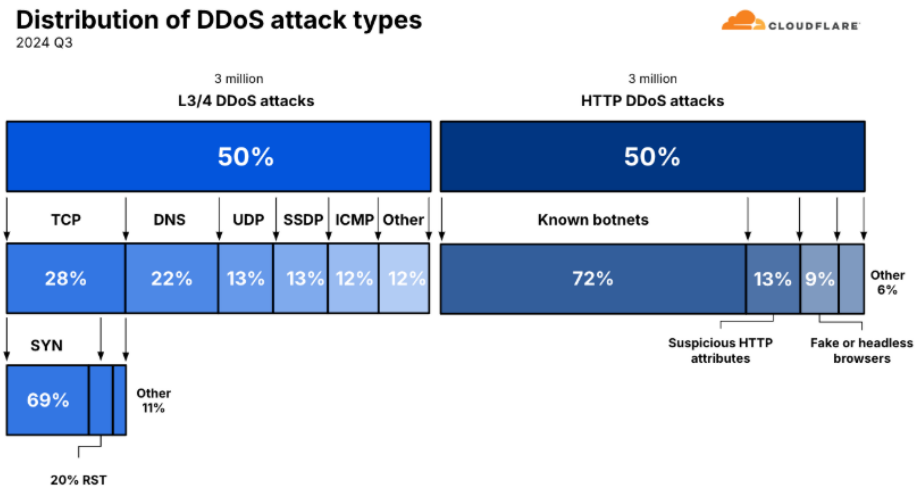
5. Considerações Finais

A análise comparativa do tráfego malicioso e legítimo, sustentada pelos gráficos obtidos, revela um padrão de intrusão de grande escala, no qual a frequência de pacotes anômalos supera drasticamente a taxa de tráfego benigno. Essa discrepância comprova a insuficiência das infraestruturas tradicionais para lidar com o volume de ataques distribuídos, achado corroborado pelos relatórios da Cloudflare (Q3 2024), que apontam a ocorrência de milhões de eventos DDoS em escala global e a necessidade de mitigações capazes de operar na casa de terabits por segundo (Tbps).

Em relação aos vetores, os resultados experimentais indicam a predominância de ataques na Camada 4 (Transporte), com alta ocorrência do protocolo UDP e foco nas portas 80 e 443, evidenciando tentativas de exaustão de largura de banda e indisponibilidade de serviços *web*. Essa constatação converge com os dados da Cloudflare, que mostram a persistência dos ataques L3/L4 (TCP, UDP e DNS) e o crescimento dos ataques HTTP (Camada 7) voltados a aplicações. Além disso, as assinaturas comportamentais observadas, como fluxos de curta

duração e pacotes de saturação, refletem o mesmo padrão descrito globalmente, especialmente nos ataques do tipo SYN *Flood*, ainda predominantes em cenários hipervolumétricos.

Figura 7 - Distribuição de tipos de Ataque DDoS



Fonte: Cloudflare (2024)

Diante desse cenário, a síntese das técnicas de mitigação converge obrigatoriamente para uma arquitetura de defesa em nuvem (*Cloud Computing*) e em múltiplas camadas. O volume exige que a primeira linha de defesa seja a Absorção e Diluição do tráfego, técnica na qual o *Anycast* é central, sendo utilizado em soluções como o *Magic Transit* da Cloudflare para distribuir e neutralizar o impacto volumétrico. Complementarmente, a alta ocorrência de UDP demanda a Filtragem Rápida L3/L4 na borda, via BGP *FlowSpec*. Finalmente, para combater o comportamento do ataque, a Mitigação na Camada 7 é essencial, exigindo o uso de *Web Application Firewall* (WAF) e *Bot Management.* A Cloudflare integra essas ferramentas com inteligência artificial para analisar a duração dos fluxos e o comportamento das requisições, limpando o tráfego malicioso antes que ele consuma os recursos do servidor. Portanto, apenas a escala e a inteligência das soluções em nuvem podem conferir a resiliência necessária contra

as ameaças demonstradas pelos dados.

Referências

AKAMAI. **What is cloud computing?** Akamai. 2025a. Disponível em: https://www.akamai.com/pt/glossary/what-is-cloud-computing. Acesso em: 27 maio 2025.

AKAMAI. **O que é um ataque volumétrico?** Akamai. 2025b. Disponível em: https://www.akamai.com/pt/glossary/what-is-a-volumetric-attack. Acesso em: 6 jun. 2025.

AKAMAI. **Understanding DDoS attacks**. Akamai. 2025c. Disponível em: https://www.akamai.com/resources/ddos-attacks. Acesso em: 6 jun. 2025.

ANTONAKAKIS, M.; APRIL, T.; BAILEY, M.; BERNHARD, M.; BURSZTEIN, E.; COCHRAN, J.; SEAMAN, C. Understanding the Mirai botnet. **USENIX Security Symposium**, 2017. Disponível em: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf. Acesso em: 8 jun. 2025.

AMAZON WEB SERVICES (AWS). **Our Origins.** AWS. Disponível em: https://aws.amazon.com/about-aws/our-origins/. Acesso em: 7 jun. 2025.

BOIN, C.; GUILLAUME, X.; GRIMAUD, G.; GROLÉAT, T.; HAUSPIE, M. *A* **comprehensive survey on DDoS attacks in cloud computing: taxonomies, challenges, and future directions**. 2022. Disponível em: https://arxiv.org/abs/2208.14205. Acesso em: 12 mar. 2025.

CLOUDFLARE. **Reflections on reflection (attacks)**. Cloudflare. 2017. Disponível em: https://blog.cloudflare.com/reflections-on-reflections/. Acesso em: 6 jun. 2025.

CLOUDFLARE. **Five best practices for mitigating DDoS attacks.** Cloudflare. 2022. Disponível em: https://www.cloudflare.com/resources/assets/slt3lc6tev37/bNnFz1PMZtHvYsCWrl3n1/fe46ed61db9ee7d9e4466484d6612de7/Five-Best-Practices-for-Mitigating-DDoS-Attacks-WP.pdf . Acesso em: 12 mar. 2025.

CLOUDFLARE. **DDoS protection with Cloudflare.** Cloudflare. 2023. Disponível em https://www.cloudflare.com/resources/assets/slt3lc6tev37/2hIapovmEBdhDq0DLCuwDR/3691243ee090906900ba1a8dce7ddd45/Two_Pager_Rate_Limiting_Letter_EN-US.pdf. Acesso em: 11 mar. 2025.

CLOUDFLARE. **What is a botnet?.** Cloudflare. 2023a. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/what-is-a-ddos-botnet/. Acesso em: 8 jun. 2025.

CLOUDFLARE. **Advanced DDoS attacks and botnets.** Cloudflare. 2023b. Disponível em: https://blog.cloudflare.com/tag/botnet/. Acesso em: 8 jun. 2025.

CLOUDFLARE. **Mantis botnet launches largest DDoS attack ever recorded.** Cloudflare. 2023c.

Disponível em: https://blog.cloudflare.com/mantis-largest-ddos-attack/. Acesso em: 8 jun. 2025.

CLOUDFLARE. **DDoS threat report for 2024 Q4**. Cloudflare. 2024. Disponível em: https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/. Acesso em: 12 mar. 2025.

CLOUDFLARE. **Ataques DDoS na camada de aplicação.** Cloudflare. 2025a. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/application-layer-ddos-attack/. Acesso em: 6 jun. 2025.

CLOUDFLARE. **Ataques DDoS famosos**. Cloudflare. 2025b. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/famous-ddos-attacks/. Acesso em: 6 jun. 2025.

CLOUDFLARE. **What is a DDoS attack?**. Cloudflare. 2025c. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/what-is-a-ddos-attack/. Acesso em: 6 jun. 2025.

CLOUDFLARE. **What is an ACK flood?** Cloudflare. 2025d. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/what-is-an-ack-flood/. Acesso em: 6 jun. 2025.

CLOUDFLARE. **What is a SYN flood attack?** Cloudflare. 2025e. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/syn-flood-ddos-attack/. Acesso em: 6 jun. 2025.

CLOUDFLARE. **HTTP flood attack.** Cloudflare. 2025f. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/http-flood-ddos-attack/. Acesso em: 6 jun. 2025.

CLOUDFLARE. **How Cloudflare automatically mitigated the world's largest DDoS attack: 3.8 Tbps.** Cloudflare. 2025g. Disponível em: https://blog.cloudflare.com/pt-br/how-cloudflare-auto-mitigated-world-record-3-8-tbps-ddos-attack/. Acesso em: 6 jun. 2025.

CLOUDFLARE. **What is Anycast?** Cloudflare. 2025h. Disponível em: https://www.cloudflare.com/pt-br/learning/cdn/glossary/anycast-network/. Acesso em: 6 jun. 2025.

CLOUDFLARE. **Frequently asked questions for DDoS protection**. Cloudflare. 2025i. Disponível em: https://developers.cloudflare.com/ddos-protection/frequently-asked-questions/. Acesso em: 6 jun. 2025.

CLOUDFLARE. **DNS filtering explained.** Cloudflare. 2025j. Disponível em: https://www.cloudflare.com/pt-br/learning/access-management/what-is-dns-filtering/. Acesso em: 6 jun. 2025.

FERNANDES, E.; JUNG, J.; PRAKASH, A. Security analysis of emerging smart home applications. In: **IEEE Symposium on Security and Privacy (SP)**, p. 636–654, 2017. Disponível em: https://doi.org/10.1109/SP.2016.44. Acesso em: 6 jun. 2025.

IBM. **O que é a arquitetura de diversos locatários?** IBM. 2025. Disponível em: https://www.ibm.com/br-pt/think/topics/multi-tenant. Acesso em: 6 jun. 2025.

INTEL. **Uma visão geral dos modelos de implantação em nuvem.** Intel. 2025. Disponível em: https://www.intel.com.br/content/www/br/pt/cloud-computing/deployment-models.html. Acesso em: 2 jun. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARTIZION. ISO/IEC 27002:2013 – **Information technology — Security techniques — Code of practice for information security controls.** Genebra, 2013.

KAGGLE. **DDoS Dataset**. Kaggle. 2018. Disponível em: https://www.kaggle.com/datasets/devendra416/ddos-datasets. Acesso em: 6 out. 2025

KAGGLE. **DDoS Traffic**. Kaggle. 2024. Disponível em: https://www.kaggle.com/datasets/oktayrdeki/ddos-traffic-dataset. Acesso em: 06 out. 2025

KOLIAS, C.; KAMBOURAKIS, G.; STAVROU, A.; GRITZALIS, S. **DDoS in the IoT: Mirai and other botnets. Computer**, v. 50, n. 7, p. 80–84, 2017. Disponível em: https://doi.org/10.1109/MC.2017.201

KOPP, D.; DIETZEL, C.; HOHLFELD, O. **Flood-GNN: flooding attacks detection on IoT networks via graph neural networks**. 2021. Disponível em: https://arxiv.org/abs/2103.04443. Acesso em: 12 mar. 2025.

MICROSOFT. **What is cloud computing?** Microsoft. 2025. Disponível em: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing/. Acesso em: 27 maio 2025.

MIRKOVIC, J.; MARTIN, J.; REIHER, P. A taxonomy of DDoS attack and DDoS defense mechanisms. **ACM SIGCOMM Computer Communication Review. New York: ACM,** v. 34, n. 2, p. 39–53, 2004.

PFLEEGER, C. P.; PFLEEGER, S. L.; MARGULIES, J. **Security in computing**. 5. ed. New Jersey: Upper Saddle River: Prentice Hall, 2015.

RADWARE. **DDoS attacks history**. Radware. 2017. Disponível em: https://www.radware.com/security/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/. Acesso em: 8 jun. 2025.

SAGE NETWORKS. **Filtros BGP FlowSpec**: A solução para a segurança de redes. 2024. Disponível em: https://sagenetworks.com.br/filtros-bgp-flowspec/. Acesso em: 4 jun. 2025.

STALLINGS, W. **Effective cybersecurity: a guide to using best practices and standards.** Boston: Addison-Wesley, 2017.

STATISTA. **Number of IoT connected devices worldwide 2020–2030**. Statista, 2024. Disponível em: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/. Acesso em: 8 jun. 2025.

TIPTON, H. F.; KRAUSE, M. **Information security management handbook.** 6. ed. Boca Raton: Auerbach Publications, 2008.

TDSYNNEX. C**omo surgiu a cloud computing**. Tdsynnex. 2020. Disponível em: https://blog-pt.lac.tdsynnex.com/bid/332223/como-surgiu-a-cloud-computing. Acesso em: 27 maio 2025

THE HACKER NEWS. ***M*irai botnet launches record 5.6 Tbps DDoS attack with 13,000+ IoT devices.** The Hacker News. 2025. Disponível em: https://thehackernews.com/2025/01/mirai-botnet-launches-record-56-tbps.html#:~:text=Mirai%20Botnet%20Launches%20Record%205.6,22%2C%202025%EE%A0%84Ravie%20Lakshmanan. Acesso em: 28 maio 2025.

WHITMAN, M. E.; MATTORD, H. J. **Principles of information security**. 6. ed. Boston: Cengage Learning, 2018.

ZHANG, Q.; WANG, L.; FU, C. **The evolution of distributed denial of service (DDoS) attacks: NLP-based detection and strategic management countermeasures in modern networks.** 2024. Disponível em: https://www.suaspress.org/ojs/index.php/JETBM/article/view/v1n4a04. Acesso em: 8 jun. 2025.

João Vitor Lopes Bezerra

Lucas Jacomini Levighin

Análise de padrões de tráfego ddos em datasets públicos e sua correlação com arquiteturas de mitigação em cloud computing

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.
Área de concentração: Segurança da informação.

Americana, 02 de dezembro de 2025.

Banca Examinadora:

Clerivaldo José Roccia
Mestre
Fatec Americana "Ministro Ralph Biasi"

José Martins Junior
Doutor
Fatec Americana "Ministro Ralph Biasi"

Thaís Godoy Vazquez Macetti
Doutora
Fatec Americana "Ministro Ralph Biasi"