UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
PRÓ-REITORIA DE GRADUAÇÃO
DEPARTAMENTO DE ENGENHARIAS E TECNOLOGIA
INTERDISCIPLINAR EM TECNOLOGIA DA INFORMAÇÃO

ALAN ALMEIDA DA SILVA

UMA INVESTIGAÇÃO SOBRE O USO DE BOTNETS EM ATAQUES DE NEGAÇÃO DE SERVIÇO DISTRIBUÍDOS CONTRA INFRAESTRUTURA DE NUVEM PÚBLICA DE COMPUTADORES

PAU DOS FERROS
2023

ALAN ALMEIDA DA SILVA

UMA INVESTIGAÇÃO SOBRE O USO DE BOTNETS EM ATAQUES DE NEGAÇÃO DE SERVIÇO DISTRIBUÍDOS CONTRA INFRAESTRUTURA DE NUVEM PÚBLICA DE COMPUTADORES

Trabalho de conclusão de curso apresentado à Universidade Federal Rural do Semi-Árido como requisito parcial para obtenção do título de Bacharel em Curso.

Orientador: Prof. Dr. Walber José da Silva - UFERSA

PAU DOS FERROS

2023

S319i Silva, Alan almeida da.
Uma investigação sobre o uso de botnets em ataques de negação de serviço distribuídos contra infraestrutura de nuvem publica de computadores / Alan almeida da Silva. - 2023.
61 f. : il.

Orientador: Walber José Adriano Silva.
Monografia (graduação) - Universidade Federal Rural do Semi-árido, Curso de Tecnologia da Informação, 2023.

1. Botnets. 2. Malware. 3. Segurança da informação. 4. Computação em nuvem. 5. Cibersegurança. I. Silva, Walber José Adriano , orient. II. Título.

Ficha catalográfica elaborada por sistema gerador automáto em conformidade com AACR2 e os dados fornecidos pelo) autor(a).
Biblioteca Campus Pau dos Ferros
Bibliotecária: Erlanda Maria Lopes da Silva
CRB: 15/966

ALAN ALMEIDA DA SILVA

UMA INVESTIGAÇÃO SOBRE O USO DE BOTNETS EM ATAQUES DE NEGAÇÃO DE SERVIÇO DISTRIBUÍDOS CONTRA INFRAESTRUTURA DE NUVEM PÚBLICA DE COMPUTADORES

Trabalho de conclusão de curso apresentado à Universidade Federal Rural do Semi-Árido como requisito parcial para obtenção do título de Bacharel em Curso.

Aprovada em: 18/04/2024

BANCA EXAMINADORA:

gov.br Documento assinado digitalmente
WALBER JOSE ADRIANO SILVA
Data: 26/04/2024 20:41:51-0300
Verifique em https://validar.iti.gov.br

Orientador: Prof. Dr. Walber José Adriano Silva (UFERSA)

gov.br Documento assinado digitalmente
JOSE FERDINANDY SILVA CHAGAS
Data: 26/04/2024 21:23:33-0300
Verifique em https://validar.iti.gov.br

Examinador: Prof. Me. Jose Ferdinandy Silva Chagas (UFERSA)

gov.br Documento assinado digitalmente
JOAO BATISTA BORGES NETO
Data: 26/04/2024 21:05:41-0300
Verifique em https://validar.iti.gov.br

Examinador: Prof. Dr. João Batista Borges Neto (UFRN)

AGRADECIMENTOS

O desenvolvimento desse trabalho de conclusão de curso contou com a ajuda de diversas pessoas, dentre as quais agradeço:

Ao professor orientador, que aceitou o desafio de desenvolver o projeto, dando todo o auxílio necessário nos momentos de dúvidas.

Aos professores do curso de Tecnologia da Informação que através dos seus ensinamentos permitiram que eu pudesse hoje estar concluindo esse trabalho.

Aos meus pais, que sem dúvida alguma são meus maiores incentivadores, e em todo momento me apoiaram torcendo incessantemente por mim.

Aos meus amigos, que sempre me apoiaram e estiveram comigo durante toda minha jornada acadêmica até aqui.

RESUMO

No contexto cada vez mais digitalizado em que vivemos, os ataques de negação de serviço distribuídos (*Distributed denial of service* - DDoS) representam uma ameaça significativa, capaz de comprometer a disponibilidade e a integridade de serviços online. O presente trabalho dispõe de uma investigação sobre o uso de *botnets* em ataques DDoS contra infraestruturas em nuvem pública de computadores, com a intenção de compreender como funcionam os mecanismos desses ataques e explorar possíveis ferramentas de mitigação. Na primeira fase da pesquisa serão explorados os conceitos teóricos e fundamentais da segurança da informação, infraestrutura em nuvem e dos ataques DDoS, além também das características das *botnets* e seu papel nesses ataques. Na segunda etapa do projeto, foram feitos experimentos práticos de ataques DoS e DDoS na Amazon Web Services (AWS) utilizando instâncias, máquina virtual, para avaliar medidas de proteção com objetivo identificar e mitigar esses ataques. Os resultados que foram obtidos com esses experimentos práticos forneceram *insights* para compreender os impactos dos ataques DDoS em infraestruturas de nuvem e identificar quais estratégias são eficazes para proteger esses serviços online. Este estudo contribuiu para o avanço do conhecimento na área de segurança da informação e fornecerá orientações práticas para profissionais e organizações que utilizam serviços de nuvem pública de computadores.

Palavras-chave: Botnets. Malware. Segurança da informação. Computação em nuvem. Cibersegurança.

ABSTRACT

In the increasingly digitized context we live in, Distributed Denial of Service (DDoS) attacks represent a significant threat, capable of compromising the availability and integrity of online services. This paper conducts an investigation into the use of botnets in DDoS attacks against public cloud computer infrastructures, aiming to understand the mechanisms behind these attacks and explore potential mitigation tools. The first phase of the research will delve into the theoretical and fundamental concepts of information security, cloud infrastructure, and DDoS attacks, as well as the characteristics of botnets and their role in DDoS attacks. In the second stage of the project, practical simulations of DoS and DDoS attacks will be conducted on Amazon Web Services (AWS) instances to evaluate protection measures aimed at identifying and mitigating these attacks. The results obtained from these practical experiments will provide insights into understanding the impacts of DDoS attacks on cloud infrastructures and identifying effective strategies to protect these online services. This study will contribute to advancing knowledge in the field of information security and provide practical guidance for professionals and organizations using public cloud computing services.

Keywords: Botnets. Malware. Information security. Cloud computing. Cybersecurity.

SUMÁRIO

1. INTRODUÇÃO

Conforme o passar do tempo, é nítido que tanto indivíduos quanto empresas vêm gradualmente se tornando cada vez mais dependentes das novas tecnologias. Os sistemas de informação e comunicação são hoje, atores fundamentais no desenvolvimento econômico, social e intelectual de toda a humanidade. A cada momento que passa, presenciamos o lançamento de uma quantidade crescente de serviços na *internet*, possibilitando um acesso cada vez mais fácil e amplo a essas ferramentas. Com a rápida globalização da *internet*, já não há mais a necessidade de visitar locadoras para alugar um filme ou série, ir a bibliotecas para fazer o empréstimo de um livro ou se locomover até um supermercado para realizar compras. Devido aos inúmeros benefícios e à facilidade de acesso que a internet oferece, esta tecnologia tem atraído um público diversificado. No entanto, essa crescente presença virtual também aumenta exponencialmente o tráfego de dados e informações confidenciais de indivíduos e empresas na rede.

Ao mesmo passo em que a sociedade vai se tornando cada vez mais digital, os riscos relacionados à cibersegurança também aumentam de forma exponencial. A todo momento criminosos cibernéticos e hackers exploram as vulnerabilidades nos sistemas e infraestruturas para roubar ou comprometer dados, realizar furtos financeiros e executar ataques de negação de serviço distribuídos (*Distributed denial of service* - DDoS). Esses ataques DDoS, em particular, são altamente perigosos pois quando não tratados com a devida atenção e qualidade podem paralisar as operações de empresas, serviços online e até mesmo infraestruturas críticas, acarretando em prejuízos financeiros e minando a confiança dos usuários.

Um dos recursos preferidos por esses invasores na execução de ataques de negação de serviço distribuídos são as *botnets*, que são redes compostas por dispositivos comprometidos que podem ser controlados remotamente pelos criminosos. A disseminação de *malwares* para a criação de grandes *botnets* possibilitam que *hackers* lancem enormes volumes de tráfego malicioso para a vítima, sobrecarregando servidores e infraestruturas online. Esta pesquisa se propõe a explorar em detalhes como essas *botnets* são concebidas, operadas e como suas ações podem ter impactos devastadores sobre serviços *online*, isso tudo utilizando dos serviços e recursos de computação em nuvem para obter os resultados.

Para Mikko Hypponen (2017) as armas cibernéticas são eficazes, acessíveis e negáveis e essa é uma ótima combinação em qualquer arma. Sabendo disso, o aumento constante na variação e evolução dos ataques cibernéticos fez com que seu índice de ocorrência aumentasse proporcionalmente, isso aliado à facilidade de acesso à tecnologia, tornou a segurança cibernética uma preocupação ainda mais vital tanto para indivíduos quanto para organizações. Os danos causados pelos ataques de negação de serviço vão além das tão mencionadas perdas financeiras, abrangendo também danos à reputação e à confiança do público.

Atualmente, uma grande parte dos serviços online estão hospedados em infraestruturas de nuvem, e a tendência é que esse comportamento aumente cada vez mais, de acordo com a Gartner, até 2025 espera-se que pelo menos 85% das empresas estejam utilizando esse tipo de computação para realizar suas atividades. Com isso, ao analisar ataques DoS e DDoS direcionados a serviços hospedados em nuvem, uma gama de fatores particulares deve ser observada com atenção, como por exemplo, a natureza distribuída e altamente escalável dessas plataformas pode tanto potencializar os ataques como oferecer oportunidades para estratégias de mitigação mais eficazes.

A elasticidade dessas infraestruturas pode ser explorada de maneira que *hackers* lancem ataques super massivos, aproveitando recursos computacionais *on-demand* (serviços sob demanda de recursos de computação) para sobrecarregar servidores ou esgotar largura de banda, prejudicando a disponibilidade dos serviços online.

Por outro lado, os provedores de serviços em nuvem têm implementado medidas avançadas de segurança com o objetivo de detectar e mitigar ataques DDoS. Estratégias como detecção de tráfego malicioso, limitação de taxa de transferência de dados, o redirecionamento de tráfego malicioso e o ajuste dinâmico dos recursos vem se mostrando cada vez mais eficientes.

Nesse contexto, é imperativo compreender sobre as estratégias de prevenção e mitigação de ataques DoS e DDoS em serviços em nuvem, bem como reconhecer o papel crucial da conscientização e da colaboração entre os setores público e privado na proteção das infraestruturas digitais.

A escolha deste tema se justifica na sua elevada importância e impacto no atual contexto da segurança cibernética. A dependência crescente da tecnologia e dos serviços online por parte de todos os usuários, torna as empresas e

organizações mais vulneráveis a ataques cibernéticos, sendo os ataques de negação de serviço particularmente preocupantes. Além disso, a evolução contínua das táticas dos invasores, como a utilização de malwares para formar botnets cada vez maiores, e a alta migração de serviços para nuvens ressaltam a necessidade de entender e enfrentar essa ameaça em constante evolução e variação. Portanto, a pesquisa nesta área é crucial para reduzir riscos, proteger dados, detectar e mitigar ataques DDoS e melhorar a segurança da informação na sociedade.

1.1 Objetivos

1.1.1 Objetivo Geral

O presente trabalho tem como objetivo entender brevemente como ocorre a formação de uma botnet e como e como ela pode ser usada para disparar Ataques Distribuídos de Negação de Serviço (DDoS). Além disso, este trabalho pretende explorar esse tipo de investida em um ambiente controlado de computação em nuvem, especificamente a plataforma Amazon Web Services (AWS) realizando tentativas de ataques direcionados a serviços com o intuito de deixá-los indisponíveis. Adicionalmente, será abordada a importância da implementação de medidas e estratégias de proteção visando mitigar e prevenir os impactos causados por ataques DDoS.

1.1.2 Objetivos Específicos

a) Analisar os custos relacionados à adoção de estratégias de proteção contra ataques DDoS, levando em conta tanto os investimentos em sistemas de segurança quanto os possíveis impactos econômicos derivados de falhas na prestação de serviços;
b) Investigar diferentes tipos de ferramentas de proteção tradicionais instaladas nos servidores e softwares de aplicação, e as disponíveis na infraestrutura em nuvem para enfrentar uma variedade de ataques DDoS.
c) Desenvolver e executar uma bateria de experimentos em um ambiente controlado para avaliar o desempenho das ferramentas de proteção escolhidas contra ataques DDoS.

d) Investigar e analisar os serviços de segurança Web Application Firewall (WAF) e AWS Shield disponibilizadas pelo provedor de nuvem pública Amazon Web Services (AWS).

1.2 Metodologia

Para realizar este trabalho sobre o uso de botnets em ataques de negação de serviço distribuídos contra infraestrutura de nuvem pública de computadores e aplicá-lo de fato em nuvem, foram utilizados diversos padrões de pesquisa científica. A seguir, serão apresentadas as principais etapas e técnicas utilizadas.

Inicialmente, foi realizada uma revisão bibliográfica sobre o tema com o objetivo de identificar conceitos, abordagens e tendências relacionadas às questões de botnets, ataques DDoS, segurança da informação e estratégias de mitigação em ambiente de nuvem. A revisão bibliográfica foi realizada com base em artigos científicos, livros e relatórios técnicos relevantes, obtidos em bases de dados como Google Scholar, SBC-OpenLib e SBRC.

Posteriormente foi realizada a escolha da plataforma de nuvem sob a qual iriam ser realizadas as aplicações práticas sobre o tema, por fatores decisivos como popularidade, recursos disponíveis na universidade e compatibilidade com as estratégias de mitigação, a plataforma escolhida foi a da Amazon Web Services, com seus serviços AWS WAF e AWS Shield. Esta escolha foi feita com base nas características que o ambiente proporciona, como a presença global da AWS, sua participação de mercado e a variedade de serviços e recursos oferecidos que são de extrema relevância para a segurança cibernética.

Os experimentos foram realizados em um laboratório de testes da AWS, onde foram inicializadas instâncias, que são máquinas virtuais na nuvem AWS, com o sistema operacional Ubuntu Server 22.04. Esses serviços fizeram os papeis de servidor, cliente e atacante(s) durante toda a etapa prática do projeto. Os experimentos foram detalhados em forma de gráficos e discutidos ao longo da sessão prática do trabalho. As análises práticas foram realizadas em quatro situações diferentes:

a) Disparos de ataques negação de serviço sem mecanismos de segurança pré-configurados no servidor;

b) Disparos de ataques de negação de serviço com mecanismos tradicionais instalados no servidor;
c) Disparos de ataques distribuídos de negação de serviço ao servidor sem mecanismos de segurança pré-definidos;
d) Disparos de ataques distribuídos de negação de serviço ao servidor com proteção de serviços disponibilizados pela nuvem AWS.

2. SEGURANÇA DA INFORMAÇÃO

Na atual era digital, a segurança da informação abrange não apenas a proteção de dados, mas também a defesa de redes e sistemas contra ameaças cibernéticas à disponibilidade. Esta área desempenha um papel fundamental para manter o bom funcionamento da internet, tendo em vista que há uma série de indivíduos mal intencionados que buscam explorar vulnerabilidades na rede para atender a seus interesses pessoais. Isso, por sua vez, pode resultar em danos a outros usuários, seja de natureza moral ou financeira.

De acordo com Forouzan (2006), a função da segurança em redes pode ser resumida em assegurar que as mensagens enviadas dentro da rede cheguem ao destinatário sem alterações, verificar a autenticidade do emissor para prevenir ataques de mensagens falsas e impedir que o emissor negue o envio ou a existência da mensagem posteriormente.

Para se fazer segurança da informação é necessário que haja pessoas capacitadas e com habilidades de pensar como um atacante, prevendo as diversas maneiras que um *hacker* pode explorar uma vulnerabilidade e tomar as medidas cabíveis da maneira mais eficiente possível.

As ameaças estão em constante evolução e estão se tornando cada vez mais complexas, a falta de conhecimento na área de segurança da informação pode ter como resultado consequências irreversíveis para uma organização, por isso é de suma importância garantir aspectos como disponibilidade, integridade, confidencialidade, autenticidade e entre outros.

Para Peter G. Neumann (1994), a segurança da informação não é um problema que pode ser resolvido por qualquer pessoa, deve-se ter um vasto conhecimento técnico e uma abordagem sistemática para sanar impasses.

Atualmente, as principais ameaças aos sistemas e dados na internet se dão por meio de *malwares*, vírus, *worms*, engenharia social e entre outros métodos. Por ser uma atividade contínua, a segurança contra essas técnicas também está em constante evolução. É importante ter conhecimento das ameaças recentes e tendências na *web* para adaptar as regras de segurança e estratégias de acordo.

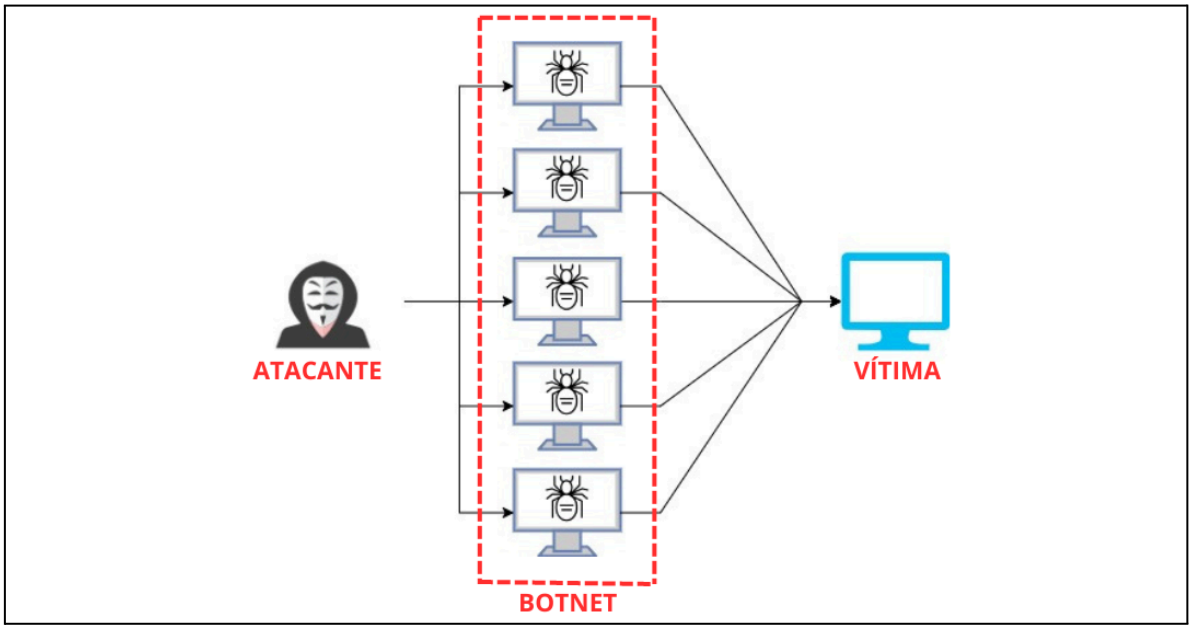
A infecção de máquinas, em sua grande maioria das vezes, acontece de maneira silenciosa, portanto é de difícil identificação. Caso a infecção ocorra com

sucesso, o atacante tem total controle da máquina da vítima e pode utilizá-la para seus interesses pré-programados.

Uma vez em posse de um dispositivo, o atacante pode usá-lo para orquestrar ataques DoS juntamente a outros aparelhos infectados, as *botnets*, que ampliam ainda mais a necessidade de robustez nas estratégias de segurança da informação.

De acordo com o conceito de DDoS, diferente de ataques DoS, eles envolvem a coordenação de múltiplos dispositivos para sobrecarregar simultaneamente um alvo específico (conforme a figura 1). Nesse contexto, a função tradicional da segurança da informação de assegurar a integridade e autenticidade das mensagens torna-se desafiadora, pois os sistemas são inundados por tráfego malicioso, comprometendo a disponibilidade dos serviços.

Figura 1 - Imagem Ilustrativa de um Ataque DDoS



Fonte: Autoria própria (2023).

Forouzan (2006), ao discutir segurança em redes, talvez não antecipasse completamente o cenário atual, no qual os ataques DDoS emergiram como uma ameaça significativa. Garantir que as mensagens cheguem sem alterações e autenticar o emissor são vitais, mas, diante de um ataque DDoS, o foco também se estende à capacidade de manter a infraestrutura online operacional frente a um volume massivo de requisições fraudulentas.

As descobertas do Relatório de Ameaças de DDoS do primeiro semestre de 2023 revelam que houve cerca de 7,9 milhões de ataques de Negação de Serviço Distribuído durante esse período, mostrando um aumento de 31% em comparação com o ano anterior, conforme relatado pela NETSCOUT.

O Brasil mantém sua posição de liderança no *ranking* de ataques na América Latina, tanto em número de ataques quanto em largura de banda, registrando 919 Gb/s. O total de ataques na região aumentou em 8% em comparação com o segundo semestre de 2022. Além disso, o país emergiu como uma das principais fontes de ataques, ocupando o segundo lugar no Top 5 de origens de ataques DDoS, com 10,3%, ficando atrás apenas dos Estados Unidos, que detêm 26,5%.

A reação a ataques DDoS exige tanto a capacidade de especialização técnica quanto a estratégias avançadas de mitigação, considerando a natureza distribuída desses ataques, a escalabilidade e flexibilidade proporcionadas pelos provedores de nuvem têm sido exploradas como uma linha defensiva eficaz. Provedores de nuvem podem facilmente redirecionar o tráfego malicioso, absorver o impacto, além de implementar medidas reativas e proativas para minimizar o impacto das operações DDoS.

2.1 Cibersegurança e sua Importância na Era Digital

Quando falamos sobre ataques na *internet*, podemos citar inúmeras maneiras em que usuários maliciosos utilizam para comprometer um serviço ou acessar algum dado específico, pode-se resumir essas ações criminosas na internet como ataques cibernéticos, ou seja, são um conjunto de ameaças em execução.

A cibersegurança é uma das áreas da segurança da informação, voltada para proteção de redes, sistemas, dispositivos e dados contra ataques e acessos não autorizados, é nesse setor que estão os profissionais responsáveis por mitigar e se proteger contra ataques cibernéticos.

Dentre os diversos ciberataques podem ser citados ataques de *malwares, phishing, hacking*, ataques de negação de serviço, entre outros. Ataques geralmente ocorrem por diversos objetivos, visando diferentes alvos e usando diferentes técnicas. Qualquer serviço, dispositivo computacional ou rede acessível através da internet está suscetível a ser alvo de um ataque, da mesma forma que qualquer

computador conectado à internet tem a capacidade de participar de um ataque (Comitê Gestor Da Internet No Brasil, 2012).

Se um invasor consegue violar dados de uma empresa, ele pode gerar custos significativos para a mesma, incluindo gastos com recuperação, perda de renda, despesas legais e danos à imagem. De acordo com o Relatório de Custo de Violação de Dados da IBM, o custo médio global relacionado a incidentes de segurança em 2023 alcançou a marca de US$4,45 milhões, registrando um incremento de 15% em um intervalo de três anos.

De acordo com John Chambers (s.d), há duas categorias de empresas: aquelas que foram hackeadas e aquelas que não sabem que foram hackeadas, isso mostra que a segurança cibernética é uma questão contínua para todas as empresas, já que nenhum sistema é completamente seguro e eventualmente podem sofrer com tentativas de ataques cibernéticos.

Para garantir a segurança, é possível implementar várias técnicas e estratégias para defender sistemas, redes e informações. Alguns dos métodos mais comuns são a utilização de *firewalls*, antivírus, criptografia, sistemas de autenticação, aplicação de políticas de segurança, treinamento de conscientização para usuários, entre outros.

Com o avanço da tecnologia e a crescente dependência das organizações em sistemas computacionais, a relevância de se fazer cibersegurança tem aumentado consideravelmente. Pessoas, organizações e autoridades devem adotar medidas eficazes de segurança cibernética para preservar seus bens digitais e garantir a confiança em seus serviços online.

2.1.1 Disponibilidade

A disponibilidade garante que a informação estará disponível quando for necessário acessá-la por pessoas autorizadas (NORMA ISO/IEC 27001:2013).

2.1.2 Integridade

A integridade é a qualidade que assegura que a informação não foi modificada indevidamente ou não autorizadamente, preservando, assim, sua consistência e integridade (NORMA ISO/IEC 27001:2013).

2.1.3 Confidencialidade

A confidencialidade refere-se à característica de proteger as informações contra acesso e divulgação não autorizados, garantindo que somente indivíduos autorizados possam visualizar os dados (NORMA ISO/IEC 27001:2013).

2.1.4 Autenticidade

A autenticidade é essencial para o acesso, exigindo autenticação para garantir que apenas usuários ou grupos autorizados possam acessar conteúdos confidenciais, está relacionada a verificação da origem genuína dos dados e a prevenção de manipulações (NORMA ISO/IEC 17799:2005).

2.1.5 Não Repúdio

O princípio de não repúdio refere-se a impedir que um usuário negue ter autoria de uma determinada informação, garantindo que tanto o emissor quanto o destinatário não possam questionar qualquer troca de informações realizada por eles (NORMA ISO/IEC 17799:2005).

2.2 Infecção de Máquinas e Formação de Botnets

Uma *botnet* pode ser resumida a uma rede de dispositivos comprometidos, geralmente infectados por algum *malware*, e que são controlados remotamente por um atacante conhecido como *botmaster*. Essas redes são usadas para executar diversas atividades maliciosas, incluindo ataques distribuídos de negação de serviço.

Os atacantes utilizam várias técnicas para transformar dispositivos em *bots* em suas atividades maliciosas, formando as suas *botnets*. Esses *bots*, uma vez infectados, realizam automaticamente tarefas para atingir objetivos maliciosos. Uma das principais técnicas empregadas pelos invasores é o uso de *malwares*, como *worms* e *trojans*. De acordo com relatório da Kaspersky Lab, no primeiro semestre de 2018 foram examinadas mais de 150 famílias de *malware* e suas modificações, que circulam por 60 mil *botnets* em todo o mundo.

Esses *softwares* maliciosos são desenvolvidos para infectar dispositivos, permitindo acesso remoto e a execução de atividades maliciosas pelos atacantes. Existem várias maneiras de tomar controle de um dispositivo e geralmente elas acontecem de maneira silenciosa, ou seja, o usuário nem chega a perceber que que seu aparelho está sendo usado por outra pessoa com objetivos maliciosos.

Para maximizar seus resultados, os agentes maliciosos infectam e tomam posse de diversos dispositivos, criando assim uma rede de aparelhos que podem ser usados a qualquer momento para executar ações nocivas contra diversos tipos de vítimas, essas redes de bots são comumente chamadas de *botnets*.

Os invasores utilizam uma variedade de técnicas para converter dispositivos em *bots* e incorporá-los a uma *botnet*. Essas técnicas geralmente exploram vulnerabilidades nos sistemas, falhas de segurança ou manipulação de usuários. Entre os principais métodos podemos citar:

a) Malwares

Os *malwares* são *softwares* maliciosos projetados com intenções maliciosas que podem variar desde roubo de dados até a interrupção do funcionamento normal de sistemas (NORMA ISO/IEC 27032:2012). No contexto de *botnets*, os *malwares* são utilizados para infectar um dispositivo e tornar possível o acesso ou execução de atividades maliciosas por atacantes remotamente.

Os principais *softwares* dessa natureza são os *worms*, um tipo de *malware* que se autoreplicante, ele faz várias cópias de si mesmo e infecta outros dispositivos desprotegidos que se conectem a máquina originalmente infectada, e os trojans que são *softwares* disfarçados de programas legítimos, muitas vezes até correspondem às funcionalidades do programa original, mas são projetados para, na verdade, dar acesso da máquina ao atacante.

b) Exploits

De acordo com Thiago e Marcelo (2021) *exploits* são técnicas, códigos ou sequências de comandos projetados para aproveitar vulnerabilidades em *software*, *hardware* ou sistemas operacionais, permitindo que um atacante ganhe acesso não autorizado, execute código malicioso e contorne medidas de segurança em sistemas de computadores, aplicativos e outros eletrônicos, como roteadores e celulares.

c) Engenharia social

A engenharia social é uma técnica utilizada por criminosos virtuais para persuadir usuários inexperientes a fornecer dados confidenciais, infectar seus computadores com *malware* ou clicar em *links* maliciosos (Thiago e Marcelo, 2021). No âmbito da segurança da informação, refere-se à manipulação psicológica das pessoas com o objetivo de induzi-las a realizar ações prejudiciais, divulgar informações confidenciais ou instalar *softwares* indevidos.

d) Dispositivos IOT (*Internet of things*)

Aparelhos como câmeras de segurança, babás eletrônicas, *smartwatches* e drones são apenas alguns entre os dispositivos chamados de IOT. Esses utensílios muitas vezes têm configurações de segurança fracas, com isso os atacantes exploram senhas padrão ou falhas de segurança para assumir o controle desses dispositivos (Alves, Peixoto e Rosa, 2021).

2.2.1 Formação de Botnets e Atividades Cibercriminosas

Uma *botnet* é construída por meio de um processo complicado e de vários estágios, que vão desde a infecção inicial dos dispositivos até o estabelecimento de uma rede de *bots* controlada remotamente. Sua arquitetura é projetada para permitir o controle remoto de um grande número de dispositivos comprometidos pelo operador da *botnet*.

Os criadores de *botnets* fazem uma seleção de potenciais alvos, com o objetivo de incluir a rede, uma ampla gama de dispositivos conectados à *Internet*. Dentre esses alvos, servidores se destacam como destinos atraentes devido ao seu poder de processamento e ao potencial de exploração de sua largura de banda para a realização de ataques DDoS. Devido a grande quantidade de dispositivos IoT e, muitas vezes, a falta de segurança adequada referente a eles, acabam se tornam alvos fáceis, podendo ser explorados para integrar uma rede de *bots*.

Além disso, computadores de uso pessoal também são constantemente integrados às *botnets*. A inclusão desses diversos tipos de dispositivos na mira dos criadores das botnets reflete a procura de uma infraestrutura diversificada, permitindo à *botnet* realizar uma gama mais ampla de atividades maliciosas e até maximizar os ganhos para os cibercriminosos.

De acordo com Tim Tan (2024), os criminosos cibernéticos desenvolvem ou adquirem *malware* específico para a criação de uma *botnet*, empregando diversas técnicas para distribuir a infecção nos dispositivos alvo. Este *malware* é criado usando técnicas avançadas para contornar as defesas de segurança das vítimas. O objetivo primário do *malware* é transformar os dispositivos visados em *bots*, equipando-os com funcionalidades controláveis remotamente pelos cibercriminosos.

Estas funcionalidades podem incluir a capacidade de realizar ataques coordenados, espalhar-se para outros sistemas, recolher e filtrar dados sensíveis, participar em campanhas de *spam*, entre outras atividades maliciosas. Segundo o relatório da Kaspersky, o *malware* pode ser disseminado de várias maneiras, incluindo anexos maliciosos em e-mails, *download* de programas não confiáveis, *links* para sites comprometidos ou exploração de vulnerabilidades em *software* desatualizado.

Após a distribuição, o *malware* inicia o processo de infecção nos dispositivos alvo, empregando uma série de técnicas sofisticadas para explorar vulnerabilidades de segurança. Ele pode ser projetado para explorar diversos tipos de vulnerabilidades, como aquelas relacionadas a protocolos de comunicação, configurações de segurança incorretas, falhas de *software* ou até mesmo a ausência das atualizações de segurança mais recentes. Depois que uma vulnerabilidade é identificada, o *malware* emprega métodos específicos para obter acesso não autorizado ao sistema alvo, que podem incluir técnicas como injeção de código, execução remota de comandos ou até mesmo sequestro de credenciais do usuário.

Após infectar com sucesso os dispositivos alvo, o *malware* estabelece uma conexão com os servidores de C&C, que são operados pelos criminosos cibernéticos. Por meio dessa conexão, os criminosos têm a capacidade de enviar comandos específicos aos robôs, instruindo-os a realizar diversas atividades maliciosas. Esses comandos podem envolver a realização de ataques DDoS, a propagação para outros sistemas, a coleta de dados confidenciais, a distribuição de *software* adicional ou qualquer outra ação programada por cibercriminosos.

Além de transmitir instruções, os servidores de C&C realizam a coleta de dados sobre os *bots*. Isto inclui informações sobre a eficácia de atividades maliciosas, a detecção de defesas de segurança, detalhes sobre o ambiente operacional dos dispositivos infectados e outras métricas importantes.

Assim que os cibercriminosos ganharam controle total sobre os dispositivos comprometidos através da *botnet*, poderão iniciar uma série de atividades maliciosas que estejam alinhadas com os seus objetivos e interesses criminosos (Luiza Pires, 2024). Conforme anteriormente discutido, uma *botnet* pode ser utilizada (entre outras atividades) para lançar ataques DDoS em serviços de *Internet*. A quantidade de funções que uma *botnet* pode realizar destaca a versatilidade desta infraestrutura para ser usada em várias formas de crime cibernético.

A capacidade de adaptar as operações da *botnet* de acordo com as necessidades permite que os cibercriminosos otimizem seus ganhos e impactos, representando uma ameaça significativa à segurança digital. A prevenção e a detecção destas atividades exigem estratégias sofisticadas de cibersegurança, além de monitoramento constante.

2.3 Arquitetura de Uma Botnet

As *botnets* podem ter diferentes tipos de arquiteturas, ela pode variar conforme o propósito para qual foi criada, além de ter a característica de crescer constantemente. Apesar dos diferentes tipos e propósitos, geralmente uma botnet é composta pelos seguintes elementos:

a) Botmaster

É o indivíduo responsável por controlar toda a *botnet*. Essa pessoa é a responsável por infectar os dispositivos que farão parte da rede bots e estabelecer os canais de conexão para enviar comandos e realizar a troca de informações.

b) Bots

São os dispositivos que foram infectados e que fazem parte da *botnet*. Esses dispositivos podem ser computadores, servidores, dispositivos IOT, celulares e quaisquer outros aparelhos conectados à *internet*.

c) Canal de comunicação

É o meio que o *botmaster* usa para se comunicar com os dispositivos infectados, os *bots*. A comunicação com os aparelhos pode ser realizada desde um servidor central, na qual podem utilizar os protocolos HTTP, IRC ou até mesmo HTTPS. No entanto, a conexão comunicação pode acontecer do tipo P2P (*peer-to-peer*), aproveitando-se do fato que todos os *bots* possam atuar como clientes ou servidores, dificultando assim a desarticulação das *botnets*.

d) Malware

O *software* responsável por infectar os dispositivos e transformá-los em bots é conhecido como *malware*. Esse *software* é encarregado de tarefas como ocultação e auto-replicação na maioria das vezes, além de persistir no sistema alvo por um longo tempo.

e) Servidores de Comando e Controle (C&C)

São servidores que atuam como um centro de comando para máquinas comprometidas em uma *botnet*. Um invasor usa o C&C para enviar instruções e receber dados de dispositivos comprometidos. Os servidores de C&C podem ser hospedados em locais físicos ou em infraestrutura de computação na nuvem para tornar a *botnet* mais resiliente.

Esses elementos juntos são os principais componentes de uma *botnet*, com eles é possível formar uma arquitetura complexa e interconectada, que permite executar uma variedade de atividades maliciosas para vários propósitos de forma eficaz.

2.4 Computação em Nuvem

Segundo Tarina Lemmi (2023) a computação em nuvem, também conhecida como *cloud computing*, é um modelo de computação que utiliza a *internet* para fornecer armazenamento, serviços e poder de processamento. A tecnologia em nuvem oferece recursos *online* acessíveis de forma remota, em vez de adquirir pacotes de serviços para computadores locais ou dispositivos físicos para armazenamento de arquivos digitais.

O acesso imediato a recursos como capacidade de processamento e armazenamento é fornecido sem a necessidade de gerenciamento direto por parte do usuário, grandes conjuntos de dados são processados em servidores centrais, acessíveis a diversos usuários conectados à rede, oferecendo uma forma conveniente de acessar informações, programas e serviços de qualquer lugar do mundo, apenas com um computador conectado à *Internet*. Em contraste com a aquisição de pacotes de serviços para dispositivos físicos, a tecnologia em nuvem proporciona acesso imediato a recursos *online*.

2.4.1 Características da Computação em Nuvem

A computação em nuvem marca uma transformação na maneira como os recursos de computação, armazenamento e serviço são disponibilizados e acessados pelos usuários. Nesse sentido, compreender as características fundamentais desse modelo é crucial, pois oferece benefícios como disponibilidade instantânea conforme a necessidade, acesso remoto e capacidade de armazenamento.

2.4.1.1 Alta Disponibilidade

A alta disponibilidade significa eliminar os pontos de falha e criar redundância nos processos e equipamentos. Dessa maneira, se um servidor falha por qualquer motivo, existe outro para dar continuidade a operação. A troca é feita instantaneamente (*failover*) e o usuário nem percebe a mudança. (Saphir, 2019).

2.4.1.2 Acesso Remoto

Os usuários podem acessar os recursos da nuvem de qualquer lugar do mundo, a qualquer momento, contanto que tenham uma conexão com a *Internet* e dispositivos compatíveis. (Salesforce, s.d).

2.4.1.3 Escalabilidade

A capacidade dos recursos na nuvem pode ser facilmente ampliada ou reduzida de acordo com as necessidades do usuário, possibilitando uma utilização flexível e eficiente desses recursos. (Safetec, 2023).

2.4.1.4 Segurança

Os provedores de serviços em nuvem normalmente adotam medidas de segurança robustas, que incluem criptografia, controles de acesso e monitoramento contínuo, visando proteger os dados e sistemas dos usuários. (Microsoft, s.d).

2.4.2 Desafios de Segurança Associados à Computação em Nuvem

Embora a nuvem ofereça diversos benefícios, ela também apresenta desafios significativos em termos de proteção de dados e sistemas contra ameaças cibernéticas. Neste contexto, é crucial compreender alguns dos desafios que a *cloud computing* enfrenta para manter a integridade dos serviços *online* contra ataques DDoS.

2.4.2.1 Custo de Escalabilidade

Os ataques DDoS em geral carregam uma grande quantidade de dados, isso além de exigir uma resposta rápida e escalável por parte dos provedores de nuvem para acompanhar o rápido aumento de tráfego, também traz a tona problemas financeiros, tendo em vista que quanto mais dados transitam na rede, mais caro é para o cliente que tem seu serviço hospedado na infraestrutura *cloud*.

2.4.2.2 Identificação de Tráfego Malicioso

Muitas vezes, em um ataque DDoS o tráfego pode ser de difícil distinção entre tráfego legítimo ou tráfego malicioso de dados, quanto mais diversificados os ataques mais eles podem se assemelhar a tráfegos normais, em um ambiente de nuvem fazer essa identificação pode ser desafiador.

2.5 Ataques DDoS em Serviços Cloud

2.5.1 Impactos de Ataques DDoS em Serviços Cloud

Como já visto antes, se não controlados corretamente, os ataques DDoS representam uma ameaça séria e multifacetada para os serviços em nuvem, entre os principais podemos citar indisponibilidade de serviços, perda de receita e clientes, danos à reputação além de custos de mitigação e recuperação. De acordo com relatório da Netscout (2018) no setor de processamento de dados, hospedagem e serviços relacionados (que inclui provedores de nuvem), houve um aumento de 83% no número de ataques de ano a ano, além de crescimento de 198% no tamanho.

Inicialmente, a indisponibilidade dos serviços é o problema mais direto a ser apresentado, o que faz com que usuários legítimos tenham seu acesso afetado. Como resultado disso, tem-se perda de clientes e de receita, pois a interrupção das operações pode levar os clientes a desistirem do produto e buscar outras alternativas. Além disso, a reputação da organização pode ser prejudicada devido à percepção da falta de confiabilidade e segurança, o que impacta a imagem da empresa perante clientes, parceiros e investidores.

Os ataques DDoS também chegam a violar os serviços de forma que os custos de mitigação e recuperação também se tornam significativos, tanto financeiramente quanto em tempo dedicado, são horas de trabalho voltadas para a restauração dos serviços após o incidente.

Esses impactos combinados destacam a importância que tem tomar medidas eficazes de prevenção e mitigação contra ataques DDoS para proteger tanto os provedores de serviços em nuvem quanto seus clientes.

2.5.2 Principais Tipos de Ataques

As investidas dessa natureza podem acontecer de diversas formas, as *botnets* estão cada vez mais tecnológicas e os atacantes em constante evolução para maximizar suas chances de sucesso em atividades criminosas. Os ataques DDoS podem acontecer de várias maneiras diferentes, agredindo pontos diferentes da infraestrutura digital, cada um com suas próprias técnicas e características. Entre eles, os principais são os ataques volumétricos, ataques de exaustão de recursos e ataques de reflexão.

2.5.2.1 Ataques Volumétricos

Para Ferreira e Nogueira (2018) nesse tipo de ataque, os invasores lançam uma grande quantidade de tráfego falso com destino a rede da vítima para sobrecarregá-la. Esse tráfego em sua grande e maioria das vezes é gerado por meio de uma *botnet*, ou servidores mal configurados, o objetivo é consumir toda a largura de banda disponível da vítima, tornando os serviços inacessíveis para usuários legítimos.

2.5.2.2 Ataques de Exaustão de Recursos

Nos ataques de exaustão de recursos, os invasores têm como objetivo principal exaurir os recursos computacionais da vítima, como CPU, memória ou capacidade de armazenamento fazendo uso indevido dos protocolos de comunicação de rede ou enviam pacotes de rede malformados, esses ataques são mais direcionados e mais difíceis de detectar. Eles podem envolver ataques de força bruta, nos quais os invasores tentam acessar recursos protegidos por meio de repetidas tentativas de autenticação.

2.5.2.3 Ataques de Reflexão

Nos ataques de reflexão, é comum os invasores explorarem servidores DNS, SNMP ou NTP mal configurados para amplificar o tráfego direcionado à vítima. São enviadas requisições falsas com o endereço IP da vítima para esses servidores, que respondem com respostas muito maiores do que as solicitações originais, sobrecarregando assim a largura de banda da vítima com um volume amplificado de tráfego.

2.5.3 Ferramentas e Técnicas Utilizadas Por Botnets

Com as *botnets* sendo cada vez mais ameaçadoras e versáteis, é válido compreender quais as técnicas mais comuns os invasores usam para a adaptação de suas *botnets* a diferentes situações e ambientes de rede, bem como sua habilidade de lançar ataques de negação de serviço de maneira persistente e eficaz.

Um dos pontos mais explorados pelas *botnets* são as vulnerabilidades emergentes em sistemas, serviços e dispositivos conectados à *internet*. Os operadores das *botnets*, nesse sentido, tendem a acompanhar vulnerabilidades recém descobertas através de sites e fóruns ou então desenvolvendo suas próprias técnicas de pesquisa, de acordo com relatório da Compugraf (2020), os invasores visam a vulnerabilidade divulgada antes da implementação de um *patch* ou solução para se aproveitar dela enquanto ainda não é corrigida. Após tomar conhecimento delas, as *botnets* podem explorá-las antes que medidas de segurança sejam adotadas.

As *botnets* além de tudo, também são altamente adaptáveis a diferentes cenários, podendo alterar o tipo de ataque DDoS que está sendo disparado no momento dependendo das defesas implementadas pela vítima de tal maneira que se um alvo implementar algum tipo de medida contra ataques volumétricos, as *botnets* podem mudar para ataques de exaustão de recursos. Essa capacidade de mudar de tática permite que as *botnets* continuem a ser uma ameaça persistente, mesmo diante de medidas defensivas.

Contudo, as *botnets* não mudam apenas a forma de ofensiva, elas também são projetadas para serem resilientes e adaptáveis a medidas de desmantelamento, incluindo o *backup* de redundâncias (múltiplos sistemas, componentes ou recursos que desempenham a mesma função crítica) e *backups* para garantir a continuidade das operações, a distribuição geográfica dos servidores de C&C para evitar pontos de falha individuais, e técnicas de auto recuperação para restaurar atividades comprometidas.

Essas estratégias ressaltam a sofisticação e a adaptabilidade das *botnets*, que continuam a representar uma séria ameaça para organizações e infraestruturas de *Internet* em todo o mundo, tornando crucial que as organizações implementem medidas de segurança abrangentes e adotem uma abordagem proativa para se defenderem contra as *botnets*.

2.5.3.1 Ocultação de Atividade Maliciosa

Antes da adaptabilidade, as *botnets* também exercem técnicas para mascarar suas atividades maliciosas e continuar funcionando de maneira oculta. Para mitigar os ataques DDoS de uma *botnet* primeiro é necessário identificar a existência dessa *botnet*, o que torna mais difícil a tarefa de fazer segurança da informação.

O encobrimento de funcionalidades maliciosas pode incluir o uso de técnicas de ofuscação de código para tornar o *malware* mais difícil de ser detectado por soluções de segurança, além de alterações comportamentais que façam com que ele simule situações de tráfego legítimo evitando detecções, e por meio de manipulações de protocolo de rede é possível praticar a evasão de sistemas de detecção de intrusão. Isso pode prolongar a permanência do *malware* em sistemas comprometidos, permitindo que os invasores mantenham o acesso não autorizado e continuem suas atividades maliciosas sem serem detectados.

Outra técnica empregada por invasores para evitar a mitigação e a detecção de suas atividades maliciosas é a variação nas fontes de lançamento de tráfego utilizadas nos ataques DDoS. Isso pode incluir o uso de *botnets* distribuídas globalmente para dificultar a identificação e bloqueio do tráfego malicioso, e a utilização de endereços IP falsificados (*spoofing*) para mascarar a origem do tráfego.

Já para proteger seus servidores de C&C e sua infraestrutura, as *botnets* podem utilizar criptografias em seus canais de comunicação, tornando-os mais seguros. Isso dificulta a detecção e o rastreamento de suas atividades por parte de das equipes de segurança, tornando mais difícil a interrupção das operações da *botnet*.

2.6 Cibersegurança em Ambientes Cloud

A alta eficiência da cibersegurança em ambientes de nuvem, especialmente em relação a ataques DDoS, pode ser facilmente alcançada por meio de uma combinação de estratégias e tecnologias especializadas para proteger os recursos digitais hospedados na nuvem.

Aumentar a eficiência operacional pode reduzir o tempo de resposta a ameaças, isso pode ser feito automatizando tarefas repetitivas ou orquestrando processos de segurança. Processos rotineiros, como monitoramento de segurança, análise de *logs*, aplicação de *patches* de segurança e remediação de vulnerabilidades, podem acelerar significativamente a detecção e resposta a ameaças quando feitas automaticamente.

Além disso, também é possível integrar diferentes ferramentas de segurança em um único local para melhorar a capacidade de resposta a ameaças em ambiente de nuvem. Fazendo uma análise específica relacionada ao problema, é possível selecionar ferramentas de segurança especializadas em mitigação de ataques DDoS.

Nos ambientes de nuvem também são comumente utilizados fluxos de trabalho automatizados para cuidar de ataques DDoS, eles podem ir desde a detecção até a mitigação e recuperação, incluindo a configuração de regras e procedimentos automatizados para identificar, avaliar e responder a atividades de rede consideradas suspeitas ou maliciosas.

Para Bruna (2023), em seu artigo à Hostinger, é crucial levar em consideração a segurança e proteção dos sistemas *cloud*, pois eles podem ser vulneráveis a riscos por diversos fatores, como ataques DDoS. Além do mais, a maior parte dos riscos de cibersegurança nesses ambientes acontece quando os usuários não estão implementando as políticas necessárias de segurança na nuvem.

2.6.1 Prevenção e Mitigação de Ataques DDoS

Monitorar continuamente o comportamento da rede e implementar sistemas avançados de segurança são as principais maneiras de identificar e responder rapidamente a ataques DDoS. Isso inclui acompanhar constantemente *logs* de eventos, analisar comportamentos anômalos e detectar ameaças em tempo real.

Uma arquitetura de segurança sólida é o pilar central para reduzir significativamente o risco de vulnerabilidades. Adotar práticas de desenvolvimento seguro, incorporar princípios de segurança desde o início de ciclo de vida do projeto e políticas de acesso mínimo privilegiado são características essenciais para manter distante o risco de sofrer com ataques de negação de serviço.

Configurar os sistemas para que sejam escaláveis é algo essencial, aumentar a capacidade de rede em resposta a picos de tráfego anormal é altamente vantajoso. De acordo com Leôncio e Campos (2012) a escalabilidade diz respeito à capacidade de um sistema suportar um crescimento. A escalabilidade automática permite que os recursos de computação, armazenamento e rede sejam dimensionados dinamicamente para lidar com o aumento repentino de tráfego durante um ataque DDoS.

Para distribuir o tráfego também é possível implementar serviços de balanceadores de carga, de forma que o fluxo de dados seja espalhado entre várias instâncias. Isso ajuda a evitar a sobrecarga de qualquer recurso específico e distribui a carga de trabalho de forma mais igualitária, tornando mais difícil para os atacantes sobrecarregarem um único ponto de falha.

A utilização de serviços de mitigação de DDoS oferecidos pelos provedores de nuvem pode ser altamente eficaz, esses serviços detectam e filtram o tráfego malicioso antes que atinja a infraestrutura do cliente, mantendo os serviços em nuvem protegidos e disponíveis.

2.6.1.1 AWS WAF (Web Application Firewall)

O serviço WAF (*web application firewall*) disponibilizado pela Amazon Web Services pode desempenhar um papel crucial na proteção contra ataques DDoS, ele pode ser configurado para filtrar e bloquear tráfego malicioso antes que atinja a aplicação durante um ataque DDoS.

Fazendo a utilização desse serviço é possível criar regras personalizadas para identificar e bloquear padrões de tráfego associados a ataques DDoS, como um grande volume de solicitações de origens suspeitas. Além disso, é possível integrar o AWS WAF com outros serviços da AWS para distribuir o tráfego de entrada e reduzir a carga no serviço. (Amazon Web Services, n.d.).

No entanto, deve-se entender que o AWS WAF sozinho não é uma solução absoluta para mitigação de ataques DDoS, é recomendável combinar esse serviço com outras técnicas de segurança, como AWS Shield, que oferece a proteção adicional contra ataques DDoS de grande escala e suporte técnico dedicado para mitigação de ataques intensos.

O AWS WAF é uma parte importante de uma estratégia de defesa contra ataques DDoS na AWS, mas é essencial complementá-lo com outras medidas de segurança, especialmente para proteção contra ataques DDoS de grande escala e sofisticados.

2.6.1.2 AWS Shield

O AWS Shield é um serviço oferecido pela AWS que tem como finalidade específica proteger uma infraestrutura na nuvem contra ataques DDoS, ele garante que os serviços continuem disponíveis e funcionando normalmente. O Shield foi projetado para monitorar e filtrar continuamente o tráfego de rede, fazer a mitigação automática de ataques DDoS e escalar automaticamente para lidar com ataques de grande escala, além de poder ser integrado a outros serviços e ter um suporte técnico especializado. Existem duas camadas de proteção oferecidas pelo AWS Shield:

a) AWS Shield *Standard*: esta é uma camada de proteção que está disponível para todos os clientes da AWS de maneira gratuita, fornecendo proteção automática contra os ataques mais comuns e

menos volumosos, ajudando a mitigar os impactos e garantindo a disponibilidade dos programas para os usuários finais. (Amazon Web Services, s.d.).

b) AWS Shield *Advanced*: Esta é uma opção de proteção mais avançada e personalizada oferecida como um serviço adicional. O AWS Shield *Advanced* oferece proteção abrangente contra uma variedade de ataques DDoS, incluindo ataques de larga escala e ataques sofisticados. Ele inclui recursos como implementação de estratégias e soluções de segurança antes que um ataque ocorra, monitoramento de tráfego em tempo real e suporte técnico 24/7 de especialistas em segurança da própria AWS. (Amazon Web Services, s.d.).

3. EXPERIÊNCIA PRÁTICA E ANÁLISE DE RESULTADOS

Partindo de todos esses conceitos teóricos, podemos fazer uma análise prática do tema em um ambiente controlado de nuvem, a AWS. Através da configuração de instâncias na plataforma Amazon Web Services e da simulação de ataques de diferentes proporções, é possível observar de perto o impacto dessas investidas na disponibilidade e na performance dos serviços em nuvem.

Segundo as políticas de uso de teste de DDoS da AWS, o volume de um teste de simulação de DDoS não pode exceder 20 gigabits por segundo e o volume de pacotes do teste de simulação de DDoS não pode exceder 50.000 pacotes por segundo ao testar qualquer tipo de recurso da AWS. (*DDoS Simulation Testing Policy - Amazon Web Services* (AWS), s.d).

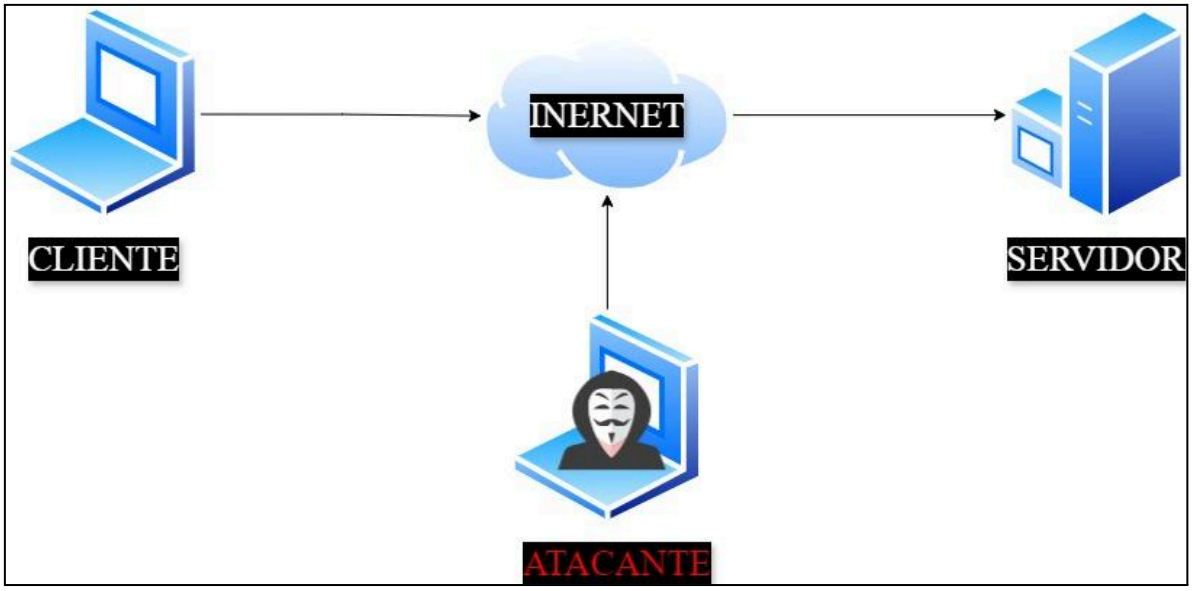
Nesse contexto, com a condução de experimentos práticos, e respeitando as políticas regulamentadoras da AWS, foi feita uma investigação comportamental, seguindo a metodologia, da reação de um serviço *web* quando exposto a um ataque de negação de serviço, sem ter nenhum mecanismo de segurança pré definido ou ferramenta de mitigação em tempo real.

3.1 Experimento de Ataques DoS no Ambiente da AWS

Para esse primeiro experimento foi utilizada a arquitetura cliente-servidor, de maneira a simplificar a compreensão de como os ataques DoS podem comprometer serviços *web*. Nesse tipo de modelo, as partes da interação são divididas entre o servidor (responsável por fornecer o serviço), o cliente (consumidor desse serviço) através da *internet*, e o atacante que irá explorar os recursos do servidor, como mostra a figura 2. Essa estrutura proporciona uma melhor organização, mas por ser um serviço centralizado é difícil fazer sua escalabilidade.

Os testes foram realizados de forma que o tempo de resposta do servidor fosse medido pela instância cliente, foram coletadas 60 amostras de tempo com 1 segundo de diferença entre cada uma delas, as medições eram feitas enquanto o ataque estivesse sendo disparado pela instância atacante. Essa abordagem permite avaliar o impacto do ataque no tempo de resposta do servidor e identificar potenciais prejuízos relacionados à indisponibilidade.

Figura 2 - Componentes da Arquitetura Cliente-servidor



Fonte: Autoria própria (2023).

Um servidor é um recurso a ser acessado dentro de uma infraestrutura que executa uma aplicação web que será acessada através da internet pelo cliente. A aplicação retornará uma página *Web* via protocolo HTTP, enquanto o cliente é o lado da conexão que solicita esses recursos e serviços, já o atacante é a parte da conexão que consome os recursos do servidor de maneira a torná-lo indisponível.

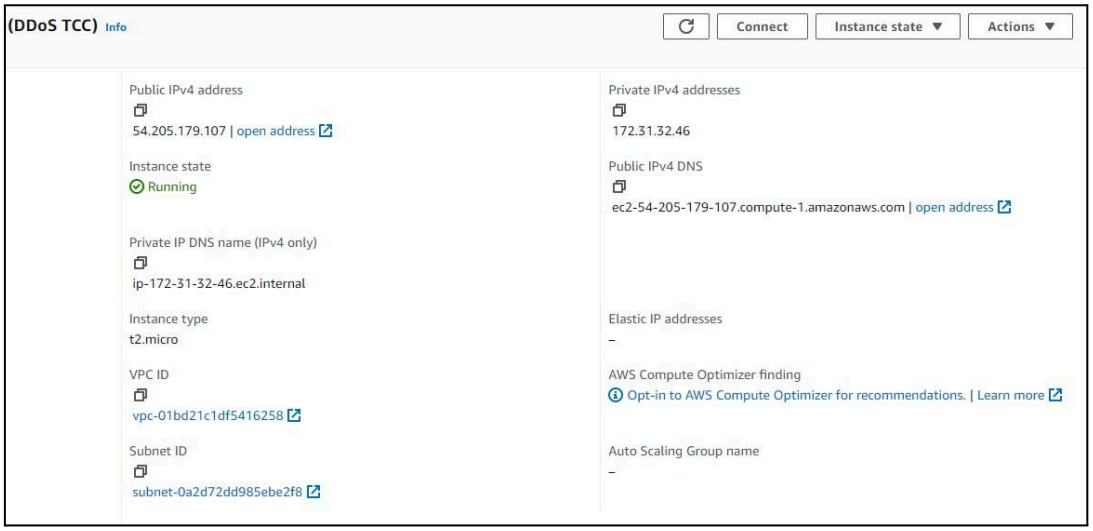
A comunicação entre eles é baseada na troca de mensagens, onde o cliente envia requisições e o servidor responde com as informações requisitadas por meio de protocolos de rede. Com essa abordagem, é possível conectar vários dispositivos a um servidor para acessar recursos privados ou compartilhados.

Para a realização do primeiro experimento, foi iniciado um laboratório exclusivo para esses testes, em seguida foram configuradas duas máquinas virtuais no serviço AWS EC2, uma delas faria o papel de servidor enquanto a outra iria realizar os ataques de maneira a simular o atacante.

Para a primeira instância, que faria o papel de vítima diante dos ataques, foram feitas configurações pontuais de forma a apenas tornar o servidor disponível na *web*, sem tratativas de segurança ou configurações adicionais. Essa instância EC2 do tipo ‘t2.micro’ (1vCPU e 1Gb memória) foi lançada no painel da AWS com o nome de “DDoS TCC”, na região Leste dos EUA (Norte da Virgínia), tendo como

sistema operacional o Ubuntu Server 22.04 LTS e com o tráfego HTTP liberado, conforme a imagem.

Figura 3 - Informações da Instância EC2 “DDoS TCC”



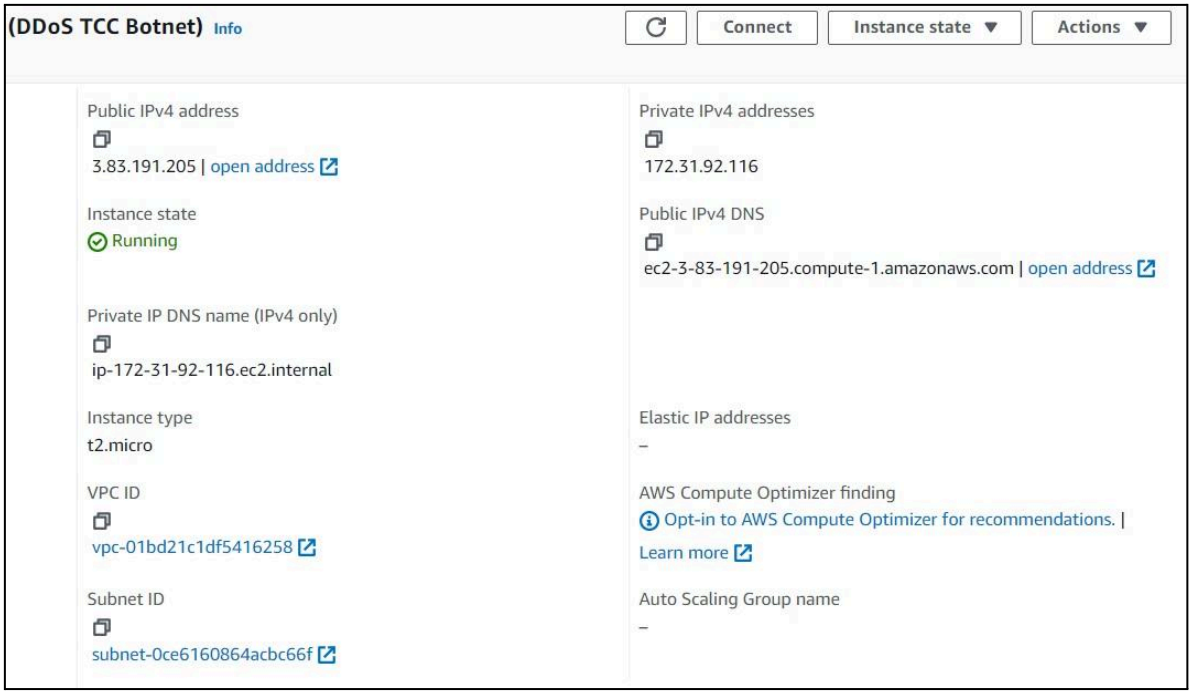
Fonte: Retirada do painel EC2 da AWS (2023).

Após o lançamento da instância, foi feita a conexão entre ela e a máquina local via protocolo SSH e executada através da chave privada. Em seguida, foi configurado o servidor *web* Apache de maneira que as páginas da *Internet* requisitadas através de um *browser* (Firefox, Internet Explorer, etc) sejam visualizadas em uma estação de trabalho, podendo ser acessada momentaneamente pelo endereço IPv4 público ‘54.205.179.107’ ou pelo endereço DNS IPv4 público: ‘http://ec2-54-205-179-107.compute-1.amazonaws.com’.

Além disso, também foi instalado o pacote Net-Tools, com objetivo de utilizar o utilitário ‘netstat’ para fazer o monitoramento das requisições em tempo real, exibindo as conexões de rede, tabela de rotas, estatísticas das interfaces entre outras informações.

Com o servidor ativo e disponível na rede, restava apenas a missão de expô-lo a ataques de negação de serviço controlados até atingir o momento de indisponibilidade do serviço. Então foi levantada outra instância EC2 do tipo ‘t2.micro’, com o nome de “DDoS TCC Botnet” na mesma região do serviço servidor, tendo como sistema operacional o Ubuntu Server 22.04 LTS, conforme a imagem.

Figura 4 - Informações da Instância EC2 “DDoS TCC Botnet”



Fonte: Retirada do painel EC2 da AWS (2023).

Com isso feito, o ambiente foi configurado de maneira a simular o atacante que irá disparar as investidas. Inicialmente foi feita a instalação da ferramenta responsável pela execução dos disparos de requisições, o slowloris (Gokturk Yaltirakli, 2015), um *software* de código aberto disponível no GitHub. Com essa ferramenta é possível direcionar ataques de negação de serviço determinando a quantidade de *sockets* que serão criados para estabelecimento de conexões com o servidor.

O slowloris funciona enviando solicitações HTTP incompletas em intervalos lentos, mantendo conexões abertas para esgotar os recursos do servidor. O ataque é disfarçado para evitar detecção e pode ser eficaz contra servidores mal protegidos.

A etapa de execução dos testes foi realizada de forma gradual, parando no momento em que o servidor ficasse completamente indisponível, ou seja, quando o tempo médio de resposta do servidor for elevado. A efetividade dos ataques foi medida relacionando a força da investida (requisições por segundo) e o tempo de resposta que a infraestrutura levava para atender as diversas requisições (em segundos).

A metodologia utilizada para medir o impacto dos ataques foi estabelecida de maneira a serem realizadas 60 análises que calcularam o tempo de resposta do site com base na quantidade de requisições feitas no momento. Foi criado um *script* para executar essas verificações periodicamente com 1 segundo de diferença de uma para a outra e cada caso de teste foi executado inteiramente duas vezes. Segue a baixo o *script* utilizado em pseudocódigo (script 1) e o gráfico de análise dos resultados (gráfico 1):

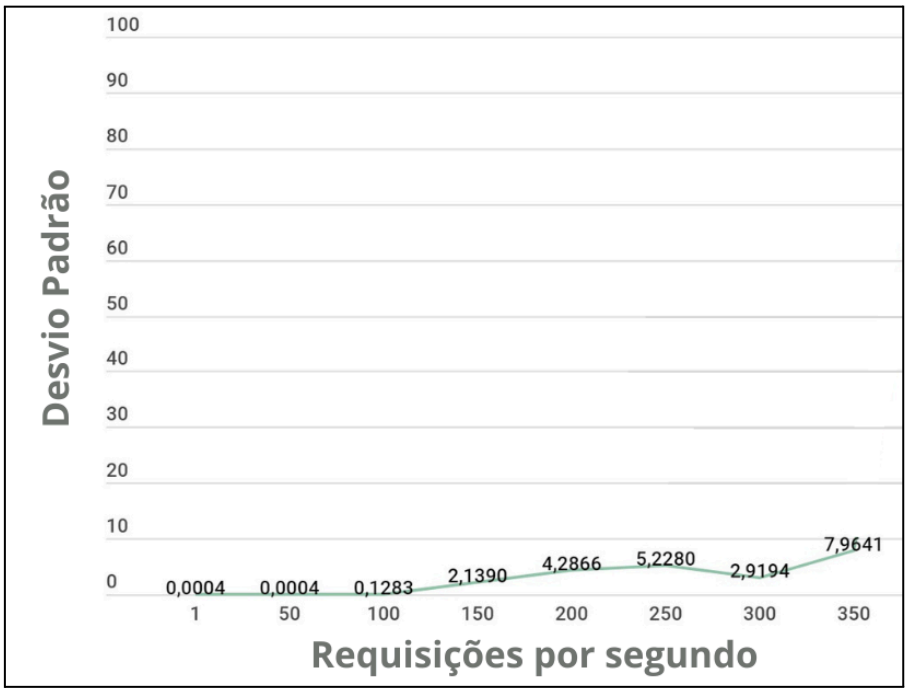
Script 1 - Código Utilizado para Medição do Tempo de Resposta do Servidor

```
#Define a URL que será testada
URL = "http://ec2-54-243-32-198.compute-1.amazonaws.com"
#Define a quantidade de vezes que serão feitos os testes
AMOSTRAS = 60
Para (i = 1 até i  = AMOSTRAS faça i++)
        #Executa o comando curl para obter o tempo de resposta da URL
           Tempo_de_Resposta = Resultado do comando curl
           #Exibe o tempo de resposta
           Exibir "Tempo de resposta: " + Tempo_de_Resposta + " segundos"
        #Aguarda 1 segundo antes da próxima iteração
        Aguardar 1 segundo
Fim Para
```

Gráfico 1 - Análise dos Dados Obtidos com os Testes DoS

Fonte: Autoria própria (2023).

Gráfico 2 - Desvio Padrão dos Dados Obtidos com os Testes DoS



Fonte: Autoria própria (2023).

Conforme mostra o gráfico 1, em condições normais, o serviço teve seu melhor tempo de resposta registrado, chegando a atingir um tempo médio de resposta de aproximadamente 0,0021 segundos. À medida que a quantidade de requisições aumentava, o servidor se mostrava cada vez mais lento em suas respostas, chegando ao ponto em que a verificação correspondente a 350 *sockets* levou quase uma hora para ser concluída. Quando o tamanho do problema foi aumentado linearmente para 400 *sockets*, o tempo de resposta não pôde ser medido, pois servidor atingiu seu ponto de indisponibilidade e o site estava inacessível.

Como visto no gráfico 2, o desvio padrão do tempo de resposta inicialmente é constante e baixo, mostrando que o servidor consegue lidar com a carga adicional de *sockets* sem oscilação significativa no tempo de resposta. No entanto, a partir de 100 *sockets*, esse desvio padrão passa a aumentar, indicando que o tempo de resposta coletado nas amostras está se tornando mais variável a cada requisição, chegando a uma margem de quase 8 segundos em 350 *sockets*, o que não é um comportamento anômalo, mas sim um insight que justifica a instabilidade do servidor *web*.

Além de analisar o gráfico de disponibilidade, também é válido fazer uma análise dos custos relacionados aos serviços com as instâncias EC2. Durante a etapa de testes dos ataques executados, os custos com os serviços das instâncias EC2 se manteve constante, porque é apenas uma instância e foi alocada por dia de uso, sendo assim, o preço final seguiu a precificação do serviço EC2 na modalidade de instâncias sobre demanda do tipo de instância t2.micro, conforme mostra o gráfico 3.

Gráfico 3 - Análise dos Custos Relacionados às Instâncias EC2

Fonte: Gerado automaticamente pelo AWS Cost Explorer (2023).

3.2 Experimento de Ataques DoS com Mecanismo de Proteção

Após terem sido feitos experimentos sem nenhum tipo de proteção à instância servidor, é válido realizar também os testes em situação de ataques DoS com uma camada de segurança pré configurada. Partindo deste pensamento, foram realizados a mesma quantidade de testes nesta etapa em relação à etapa anterior visando analisar os resultados e metrificar possíveis melhorias do servidor em resposta às mesmas quantidades de requisições. Assim, os experimentos serão realizados novamente com a adição do detalhe de haver um mecanismo de proteção contra DoS no lado do servidor *Web*.

Portanto, para estes novos casos de testes, todas as configurações originais das instâncias atacante e servidor foram mantidas, bem como a arquitetura cliente-servidor, mas foi adicionada uma camada de proteção ao serviço vítima do experimento, utilizando comandos no terminal das ferramentas sysctl e iptables do sistema operacional Linux.

O sysctl é um comando do sistema Linux que permite aos usuários do sistema visualizarem e modificarem parâmetros do kernel em tempo de execução e é frequentemente utilizado para ajustar algumas configurações de rede. Para a configuração do servidor *web* chamado “DDoS TCC”, foi utilizada uma estratégia direta à ataques de negação de serviço (*script* 2).

O iptables é uma ferramenta que permite configurar regras de *firewall* que possibilitam controlar o tráfego de entrada de dados na rede, com ela é possível manipular todo o processo de recebimento de pacotes. Neste caso, foram configuradas regras de *firewall* que limitam a taxa de pacotes SYN que o sistema pode receber, e descarta os pacotes que excedem essa quantidade (script 2).

Script 2 - Sequência de Comandos para Controlar as Requisições Recebidas

```
#Habilitando SYN cookies
sysctl -w net.ipv4.tcp_syncookies=1
#Limita a entrada de pacotes SYN
sudo iptables -A INPUT -p tcp --syn -m limit --limit 1/s -j ACCEPT
sudo iptables -A INPUT -p tcp --syn -j DROP
```

O comando “sysctl -w net.ipv4.tcp_syncookies=1” ativa a função “SYN cookies” no kernel do sistema que age como uma técnica de defesa contra ataques de negação de serviço, na etapa de estabelecimento de conexão (three way handshake). Esses cookies permitem ao sistema lidar eficientemente com a sobrecarga de conexões, respondendo aos pacotes SYN com um SYNACK contendo um número de sequência especial. Este número codifica informações relevantes, como endereços IP, portas e tempo de envio do pacote.

Assim, mesmo que a fila de conexões semi abertas esteja cheia, o sistema pode aceitar conexões legítimas. Isso é crucial em ataques de inundação SYN, nos quais invasores enviam uma grande quantidade de pacotes SYN para sobrecarregar a fila de conexões semi abertas e impedir conexões válidas. Os cookies SYN permitem que o sistema mantenha sua capacidade de resposta mesmo sob tais

ataques, garantindo a continuidade das operações. (*Ensure TCP SYN Cookies Is Enabled,* 2024).

Já os comandos da ferramenta iptables, tem como objetivo gerenciar os pacotes SYN que chegam ao servidor, o comando *“sudo iptables -A INPUT -p tcp --syn -m limit --limit 1/s -j ACCEPT”* serve para limitar a quantidade de pacotes SYN que chegam ao sistema, ele permite que apenas um pacote SYN por segundo seja aceito de uma mesma origem, enquanto que o comando *“sudo iptables -A INPUT -p tcp --syn -j DROP”* tem como objetivo descartar todos os pacotes que não forem aceitos pela regra anterior, ou seja, se o serviço receber mais de uma requisição por segundo do mesmo local, os excedentes serão descartados.

As configurações da instância atacante e a metodologia do ataque se mantiveram as mesmas, bem como o *script* usado para medir o tempo de resposta do servidor e o *software* atacante. Segue abaixo o gráfico correspondente aos dados obtidos (gráfico 4).

Gráfico 4 - Análise dos Dados Obtidos com os Testes DoS Sem Mecanismos de Proteção

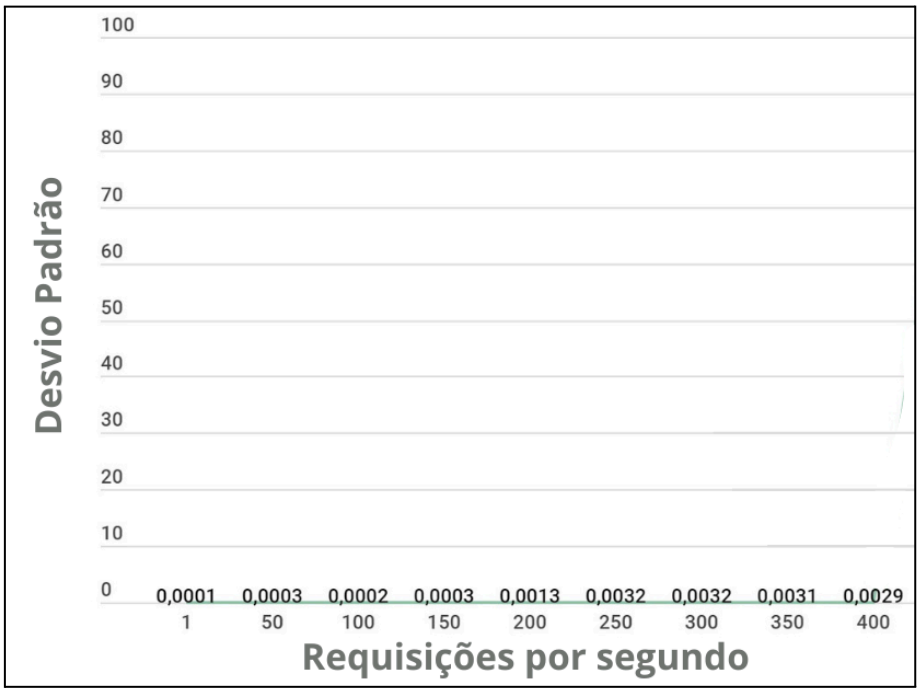
Fonte: Autoria própria (2023).

Conforme o gráfico, o serviço servidor se manteve estável e com tempo de resposta altamente superior em todos os volumes de ataques correspondentes em

relação ao gráfico do teste sem mecanismo de proteção (gráfico 1), isso se dá devido às ferramentas pré configuradas na instância servidor, que manipulam as requisições recebidas de maneira a evitar a sobrecarga dos recursos do serviço e também gerenciam a aceitação e descarte das conexões (figura 5).

No entanto, é possível notar que a partir de 250 requisições por segundo, apesar de não atingir o ponto de indisponibilidade, há um aumento brusco em relação aos tempos de resposta anteriores. Este comportamento é atribuído ao tempo de processamento necessário por parte do *firewall* para analisar individualmente cada requisição que chega ao servidor. Essa inferência se baseia na compreensão do funcionamento do *firewall*, que demanda um certo tempo para examinar e decidir o destino de cada requisição. Portanto, é plausível afirmar que esse aumento nos tempos de resposta está relacionado ao tempo de processamento do *firewall.*

Gráfico 5 - Desvio Padrão dos Dados Obtidos com os Testes DoS com Mecanismo de Proteção

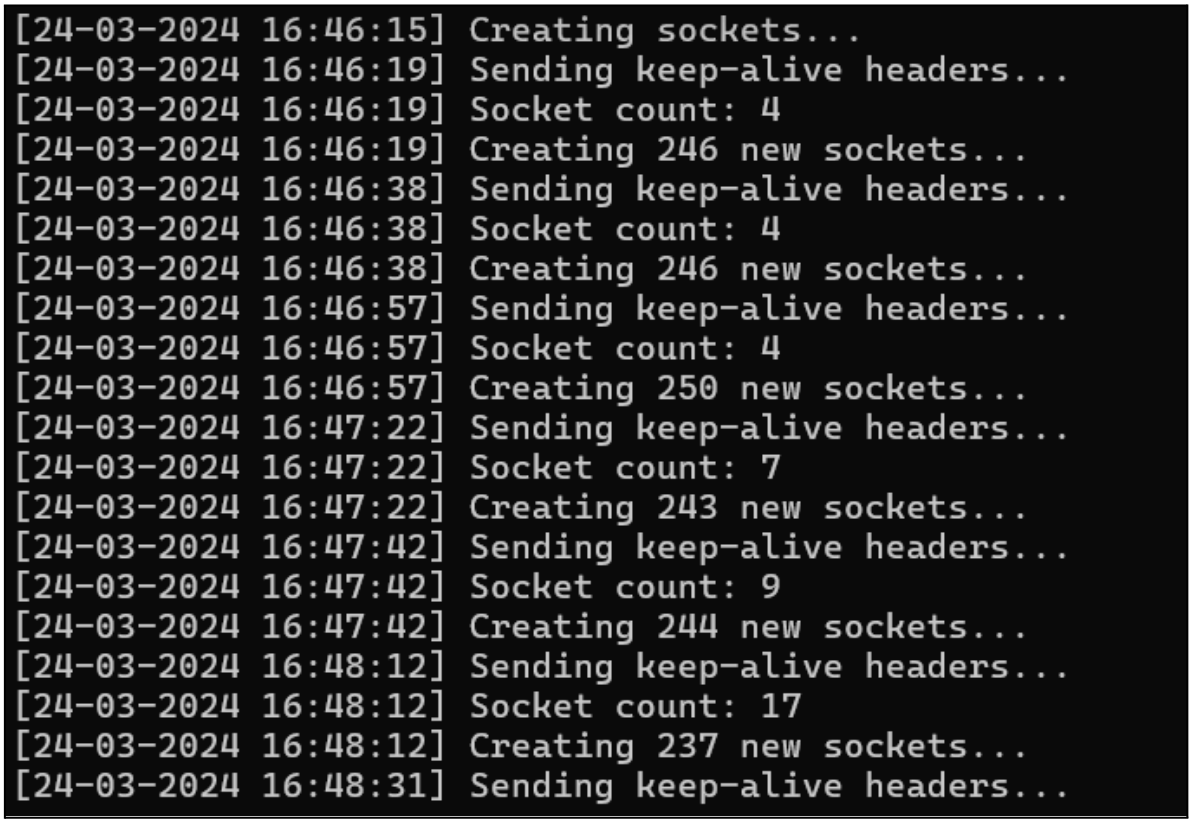


Fonte: Autoria própria (2023).

Mediante as informações do gráfico, nota-se que o servidor consegue lidar bem com as requisições feitas a ele, e o desvio padrão se mantém pequeno,

sugerindo que o tempo de resposta individual de cada requisição pelo servidor Web se manteve praticamente sem oscilações.

Figura 5 - Comportamento da Instância “DDoS TCC Botnet” Durante um Ataque

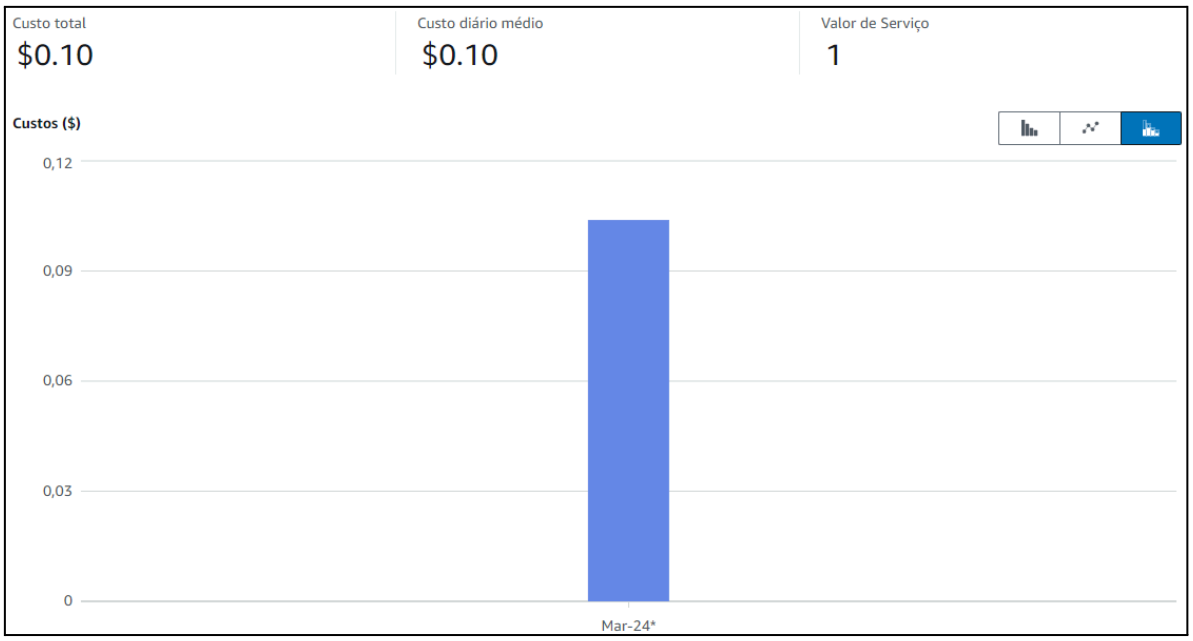


Fonte: Terminal da instância EC2 correspondente (2023).

Como pode ser observado, a quantidade de conexões foi controlada de tal maneira que o *software* atacante não pudesse direcionar a quantidade de requisições definida em seus comandos de disparo, nesse exemplo, o comando executado pelo atacante indicava um disparo de 250 requisições/s, mas devido à camada de proteção adicionada ao servidor, essas condições não foram atendidas, além também, do número de conexões direcionadas a vítima ter sido altamente inferior ao programado.

Com a disponibilidade do serviço mantida, é a vez de fazer a análise dos custos e medir se houve economia entre uma situação e a outra. Conforme o gráfico 6 mostra, o valor se manteve constante correspondente a etapa de testes anterior, mesmo com uma camada de proteção pré definida em relação ao primeiro caso onde não haviam configurações de segurança em vigor.

GRÁFICO 6 - Análise dos Custos Relacionados às Instâncias EC2



Fonte: Gerado automaticamente pelo AWS Cost Explorer (2023).

Desta vez, todos os ataques foram realizados no dia 24 de março. Conforme a imagem, é possível observar as tratativas de segurança e exigência dos serviços de *firewall* não alteraram o custo com as instâncias, que se manteve constante em relação ao gráfico anterior (gráfico 3), mostrando que é possível fazer a proteção inicial dos serviços sem ter maiores gastos ou prejuízos, mas não é suficiente para tratar de ataques mais volumosos.

3.3 Experimentos de Ataques DDoS na AWS

Com os testes de ataques DoS concluídos, é necessário realizar os experimentos com mais de uma instância atacante, para simular uma rede de *bots* e tornar o ataque distribuído. Para dar início a nova fase de experimentos, foi reiniciada a instância servidor as configurações iniciais removendo as tratativas de segurança e ferramentas de *firewall*, por meio dos seguintes comandos:

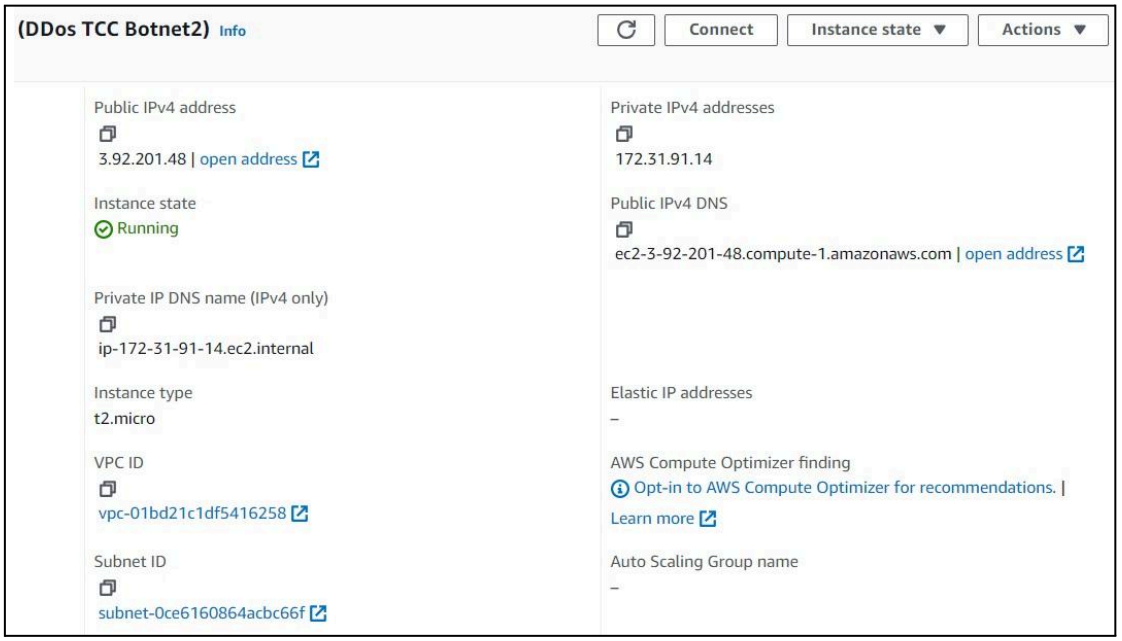
Script 3 - Sequência de Comandos para Reverter as Ações Feitas Anteriormente

```
sysctl -w net.ipv4.tcp_syncookies=0
sudo iptables -D INPUT -p tcp --syn -m limit --limit 1/s -j ACCEPT
```

sudo iptables -D INPUT -p tcp --syn -j DROP

Além disso também foi criada uma outra instância EC2 do tipo ‘t2.micro’, com o nome de “DDoS TCC Botnet2” na mesma região do serviço servidor (Norte da Virgínia), tendo como sistema operacional o Ubuntu Server 22.04 LTS, conforme a figura.

Figura 6 - Informações da Instância EC2 “DDoS TCC Botnet2”



Fonte: Retirada do painel EC2 da AWS (2023).

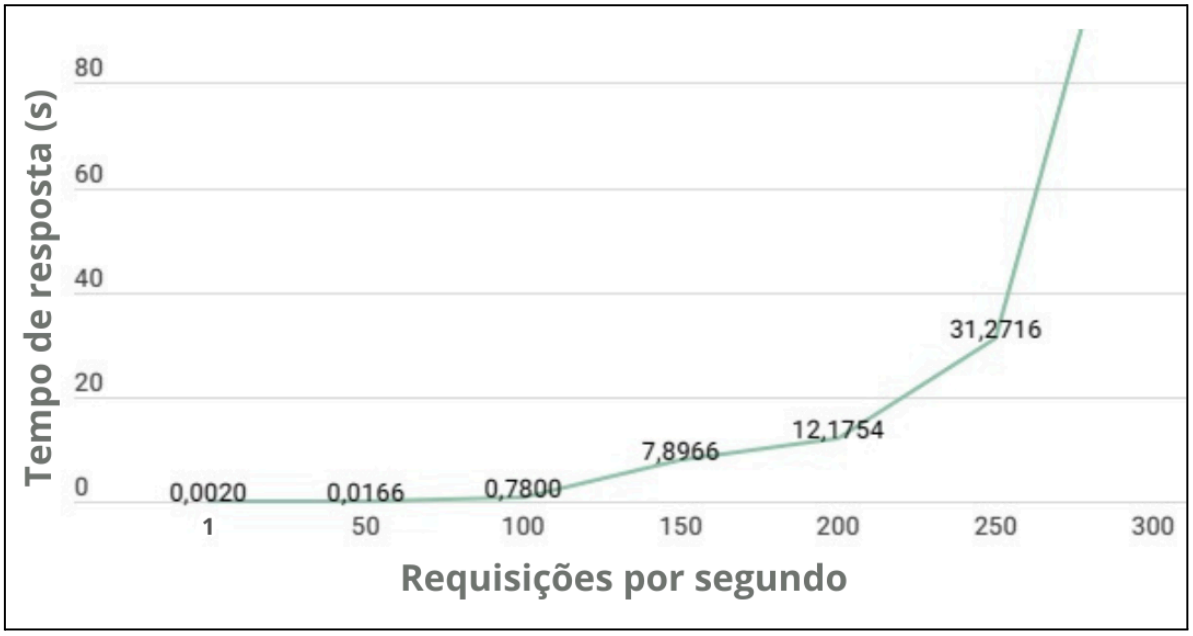
Depois de lançada, foi feita a conexão com a instância via protocolo SSH e configurado o *software* slowloris, tal qual a configuração da primeira instância atacante (DDoS TCC Botnet).

Os testes de ataques DDoS funcionaram seguindo a mesma metodologia dos testes de ataques DoS, de forma gradual e encerrados quando o servidor atingisse o ponto de indisponibilidade. A eficácia dos ataques também foi avaliada através da relação entre a intensidade dos ataques (quantidade de requisições por segundo) e o tempo que o servidor levava para responder as requisições (medido em segundos).

Para medir os impactos foi utilizado o mesmo *script* da etapa anterior (Script 1), de maneira a verificar o tempo de resposta do servidor periodicamente com 1 segundo de intervalo entre uma verificação e outra. O *script* foi executado

inteiramente duas vezes para cada caso de teste. Segue abaixo o gráfico com os resultados obtidos (gráfico 5):

GRÁFICO 7 - Análise dos Dados Obtidos com os Testes de Ataques DDoS

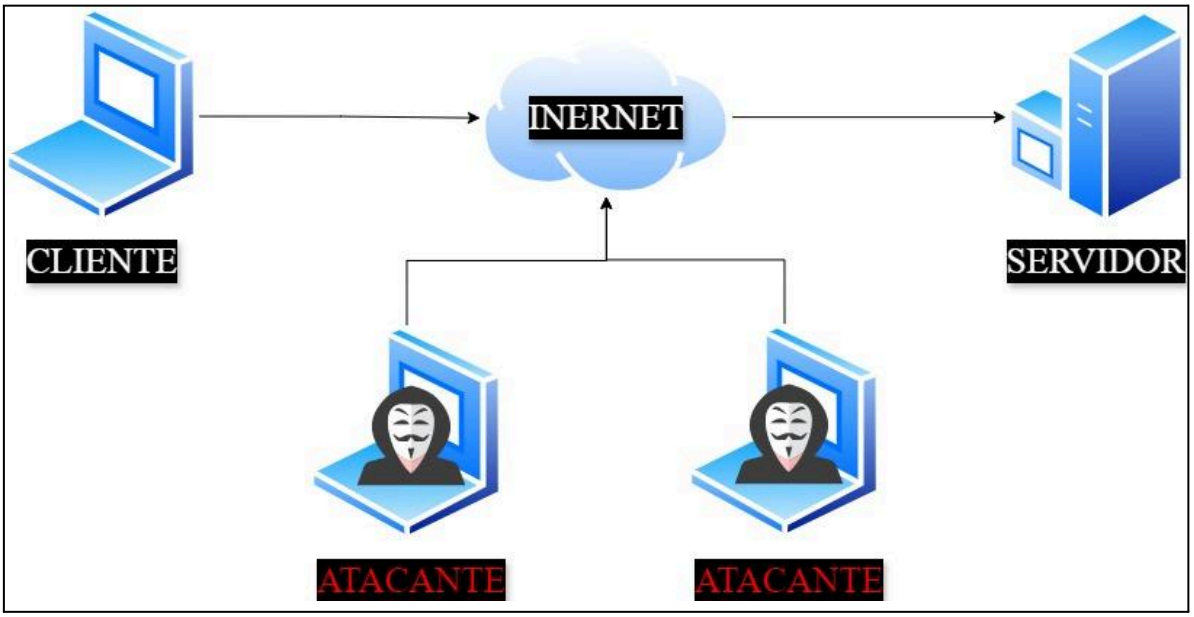


Fonte: Autoria própria (2023).

Os tempos de requisições informados na parte inferior do gráfico referem-se à quantidade lançada por cada instância atacante, ou seja, quando o valor era de 50 significa que cada uma das duas instâncias atacantes estava configurada para disparar conexões a partir de 50 *sockets*, que lançarão as requisições, e assim sucessivamente.

Conforme o gráfico, o servidor se mostrou ativo até receber 250 requisições por segundo de cada uma das instâncias atacantes (500 requisições no total conforme mostra o diagrama de arquitetura da figura 7), e ficou indisponível a partir de 300 requisições por instância (600 no total).

Figura 7 - Componentes da Arquitetura Cliente-servidor dos Testes DDoS



Fonte: Autoria própria (2023).

Analisando esses dados e comparando com o gráfico do teste anterior correspondente (gráfico 1) podemos perceber que o ponto de indisponibilidade dos dois tem 200 requisições de diferença.

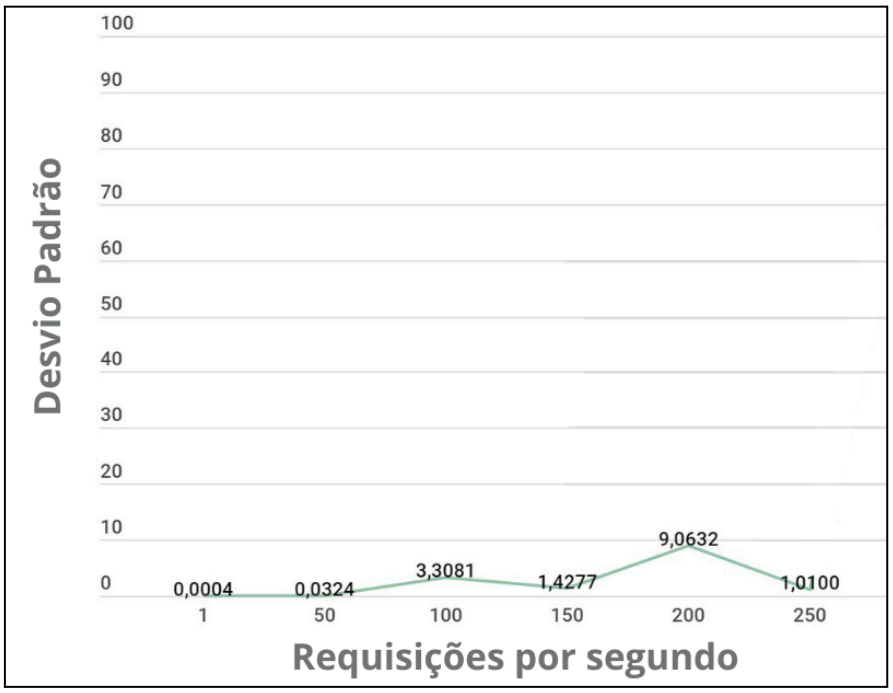
Figura 8 - Informações Sobre as Conexões da Instância Servidor

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address
tcp        0      0 127.0.0.53:53           0.0.0.0:*
tcp        0      0 0.0.0.0:22              0.0.0.0:*
tcp6       0      0 :::22                   :::*
tcp6     500      0 :::80                   :::*
```

Fonte: Retirado do terminal da instância servidor (2023).

Esse comportamento se dá devido a forma como o kernel do sistema operacional gerencia as solicitações de conexão. De modo a não prejudicar os outros processos em execução, o kernel disponibiliza apenas uma parte das suas unidades de processamento para tratar e alocar as conexões vindas da pilha TCP/IP, associadas à tupla (IP_SRC,PORT_SRC,IP_DST,PORT_DST), isso significa que para quantidades diferentes de instâncias, o sistema operacional irá dedicar uma quantidade diferente de recursos para lidar com cada uma delas de maneira que os serviços internos continuem funcionando.

Gráfico 8 - Desvio Padrão dos Dados Obtidos com os Testes DDoS



Fonte: Autoria própria (2023).

De acordo com o gráfico 8, o servidor mostrou diversos momentos de variação no tempo de resposta das requisições, tendo seu pico em aproximadamente 9 segundos quando era alvo de um ataque DDoS a partir de 200 *sockets* por atacante, o que, novamente, justifica o gráfico de análise de tempo médio de respostas, que mostra nos mesmos momentos que o servidor está lutando contra a indisponibilidade.

3.4 Experimento de Ataque DDoS com Mecanismo de Proteção

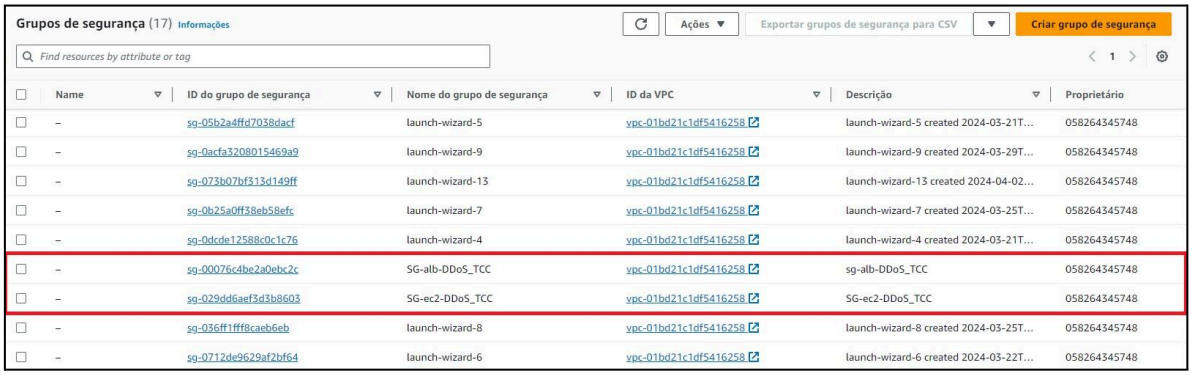
Com os testes de ataques DDoS sem nenhuma proteção direta à instância servidor, faz-se necessário a análise de ferramentas para mitigação dessas investidas, assim como seus devidos experimentos de qualidade. Sendo assim, nesta etapa foram realizados os mesmos testes da etapa anterior para analisar os resultados e representá-los graficamente visando melhorias de resposta da instância servidor as requisições solicitadas.

Para dar sequência aos testes, foram feitas atualizações na maneira como a instância servidor é protegida, foram criados *security groups, launch template*, balanceador de carga e um *auto scaling group* com a camada de proteção WAF &

Shield. Cada um desses passos teve um desempenho significativo para garantir a disponibilidade do servidor.

Inicialmente foram criados dois *security groups* separados, um para o *load balancer* e outro para a instância servidor, o que garante a aplicação de políticas de segurança específicas para cada componente do sistema, reduzindo a superfície de ataque. Além disso, foi configurada uma regra de entrada permitindo apenas que o tráfego HTTP vindo do *security group* do *load balancer* chegasse no servidor, de maneira que só ele tenha acesso direto à instância.

Figura 8 - Informações dos Security Groups Criados



Fonte: Retirada do painel de Grupos de segurança da AWS (2023).

Em seguida foi criado um *launch template* com o objetivo de padronizar a geração da instância servidor, as configurações do serviço foram mantidas em relação aos outros testes, ou seja, foi escolhida a AMI Ubuntu Server 22.04 do tipo t2.micro, além disso foi adicionado um script para que o comportamento inicial dela seja atualizar os pacotes do *software* e instalar o servidor apache2 (script 4).

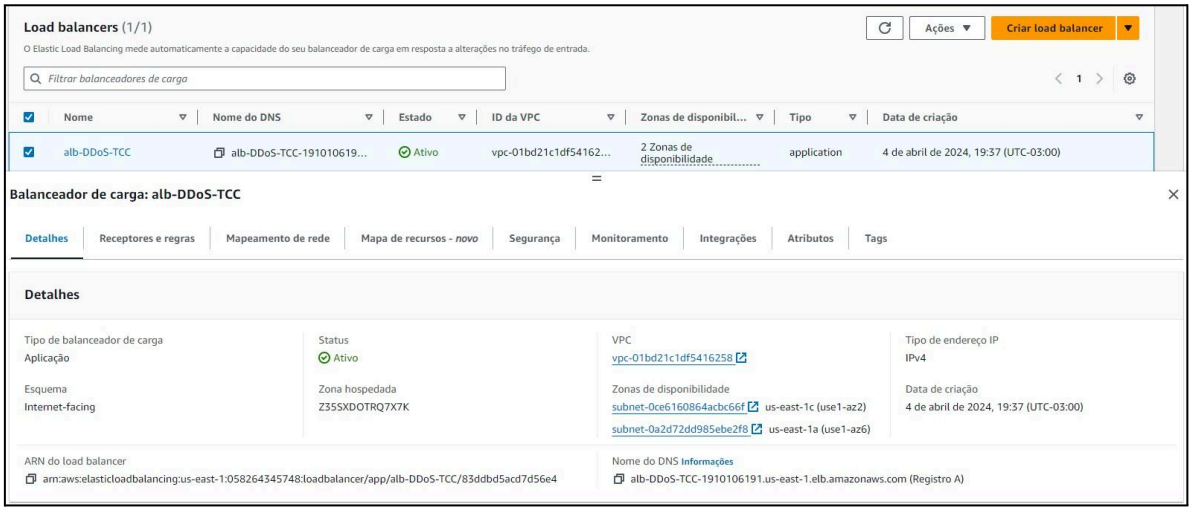
Script 4 - Sequência Utilizada para Instalar o Servidor Web Apache

```
#!bin/bash
sudo apt update -y
sudo apt install apache2 -y
```

Após isso, foi criado um balanceador de carga do tipo *Application Load balancing* para distribuir o tráfego de entrada de forma equilibrada entre as instâncias servidor, evitando assim a sobrecarga e aumentando a disponibilidade e escalabilidade do serviço. Além disso, o balanceador de carga fica responsável por

terminar as conexões, o que pode ajudar a proteger o servidor contra ataques diretos, já que o tráfego malicioso é filtrado antes de chegar às instâncias.

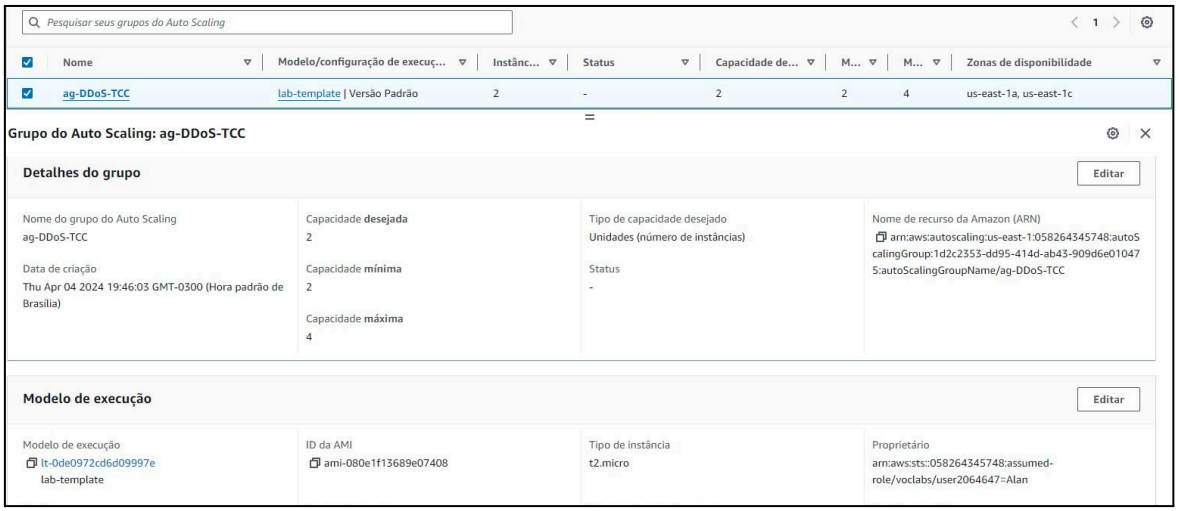
Figura 9 - Informações Sobre o Application Load Balancing



Fonte: Retirada do painel de Load Balancers da AWS (2023).

Por fim foi configurado um *auto scaling group* com o objetivo de que as instâncias sejam escalonadas automaticamente de acordo com o tráfego. Foram destinadas quantidades mínimas (2) e máximas (4) de instâncias para garantir que haja sempre a capacidade necessária para lidar com a carga de tráfego, assegurando a disponibilidade mesmo sob ataques de negação de serviço, e ao mesmo tempo evitando gastos excessivos com recursos não utilizados (figura 10).

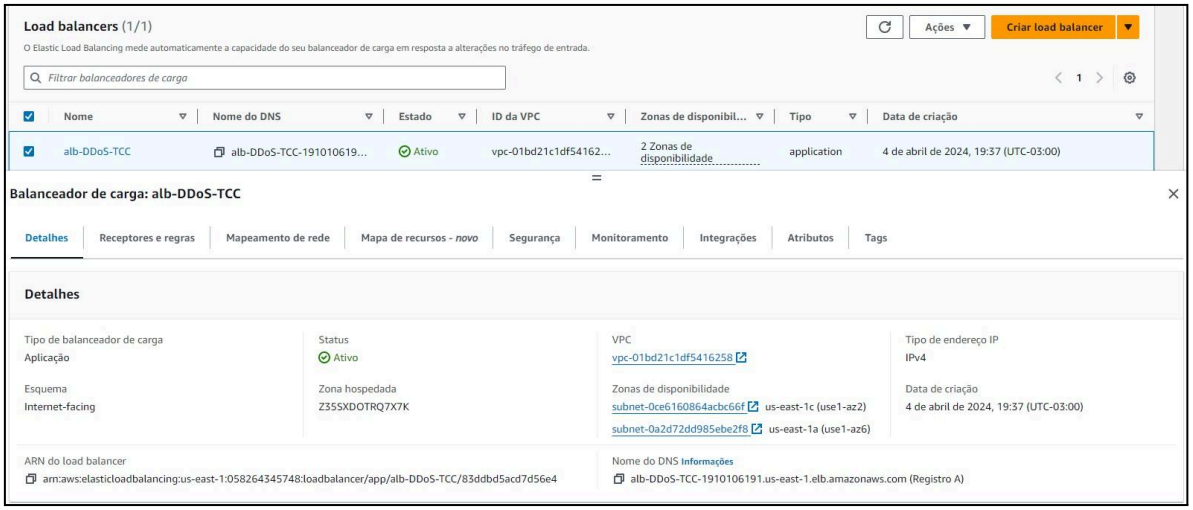
Figura 10 - Informações Sobre o Auto Scaling Group



Fonte: Retirada do painel de grupos do Auto Scaling (2023).

No *auto scaling group* também foi adicionada uma camada de proteção extra, o AWS WAF & Shield, de maneira a monitorar e filtrar o tráfego, foram também selecionadas regras para bloquear endereços IP associados a *bots* ou outras ameaças e proteger o serviço contra ataques comuns, como injeção de SQL, XSS e exploração de vulnerabilidades conhecidas (figura 11).

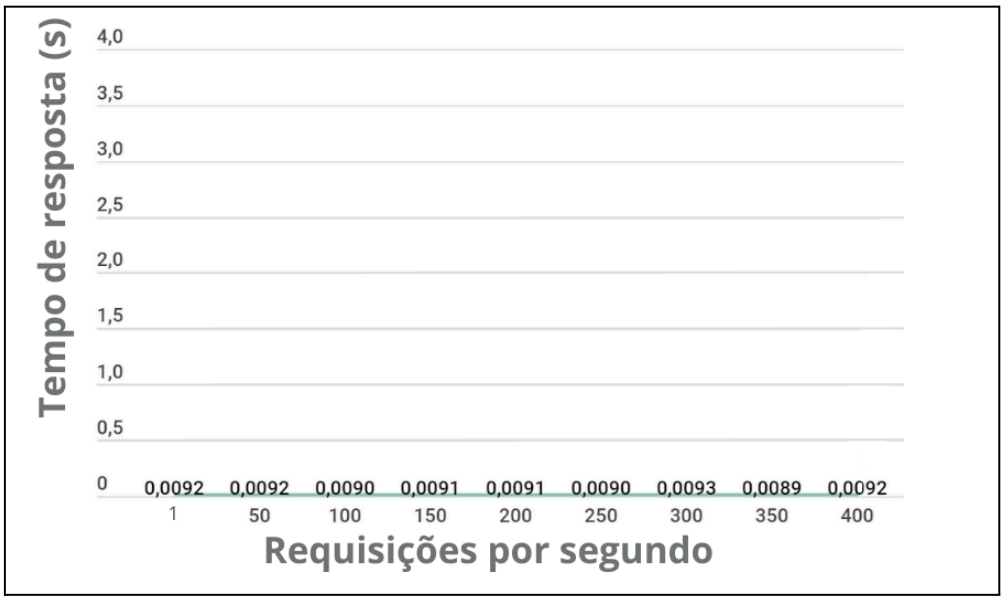
FIGURA 11 - Informações Sobre Web ACL



Fonte: Retirada do painel do serviço WAF & Shield (2023).

Após terminar as novas configurações de segurança do servidor foram direcionados os mesmos ataques pelas instâncias atacantes (que permaneceram com as mesmas configurações) com o objetivo de avaliar as ferramentas utilizadas na identificação e mitigação dos ataques DDoS, segue abaixo o gráfico com o balanço entre as requisições por segundo e o tempo de resposta dessa etapa de testes:

GRÁFICO 9 - Análise dos Dados Obtidos com os Testes de Ataques DDoS com os Mecanismos de Proteção



Fonte: Autoria própria (2023).

Conforme mostra o gráfico, o sistema se manteve estável e sem anormalidades durante todo o tempo de testes, ficando com o tempo de resposta constantemente na parte inferior da imagem, com intervalos médios de resposta variando entre 0,0089 segundos e 0,00092 segundos mesmo nos momentos em que os ataques de negação de serviço estavam sendo direcionados em larga escala ao servidor.

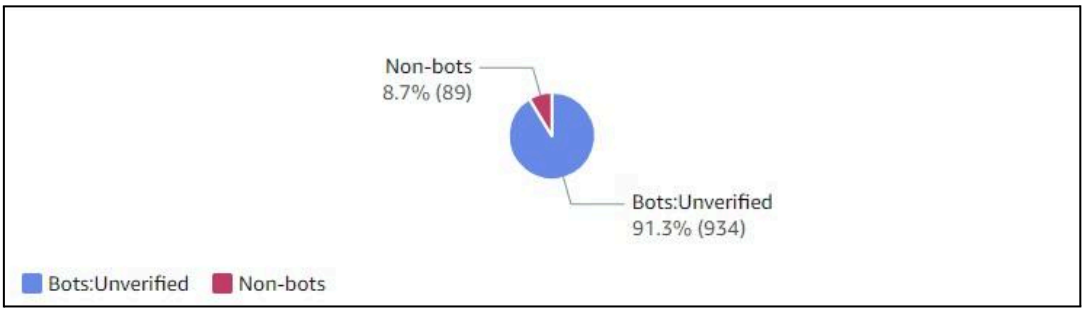
Analisando o desvio padrão (gráfico 10) e comparando-o com o gráfico de tempo de respostas correspondente (gráfico 9), percebe-se que o servidor está lidando de forma eficaz com a carga dos ataques DDoS. O desvio padrão está baixo e se mantém praticamente estável, indicando que o tempo de resposta do servidor se mantém constante mesmo quando os ataques DDoS escalam seu tamanho. O que prova que as medidas de segurança implementadas são capazes de gerenciar o tempo de resposta do servidor de maneira eficiente independente da largura da investida.

Gráfico 10 - Desvio Padrão dos Dados Obtidos com os Testes DDoS

Fonte: Autoria própria (2023).

Analisando os gráficos gerados pelo AWS WAF & Shield (gráfico 11) é possível notar que foram bloqueadas 934 solicitações que tiveram como origem *bots* não identificados, e aceitas apenas 89 solicitações, que eram requisições legítimas feitas de celulares e computadores simultaneamente para verificar, também, a disponibilidade do serviço.

Gráfico 11 - Balanço do Filtro de Tráfego



Fonte: Gerado automaticamente pelo AWS WAF & Shield (2023).

Com a disponibilidade do serviço garantida, deve-se fazer uma análise dos custos e verificar como as ferramentas influenciarão no valor médio diário. Conforme o gráfico 12, é possível notar um ligeiro aumento em relação ao gráfico anterior, isso

ocorre devido aos preços associados aos serviços em que o servidor se encontra assegurado, mas ainda não é algo muito expressivo se comparado com os benefícios absolutos que essas ferramentas de segurança trazem.

Gráfico 12 - Análise dos Custos Relacionados às Instâncias e Ferramentas

Fonte: Gerado automaticamente pelo AWS Cost Explorer (2023).

3.5 Análise dos Resultados Obtidos com os Experimentos

O experimento visou analisar os efeitos de ataques de negação de serviço (DoS) e ataques distribuídos de negação de serviço (DDoS) na plataforma da AWS, medindo o tempo de resposta para analisar a disponibilidade do servidor. Sem proteção, à medida que o volume de requisições aumentava o servidor se tornava indisponível, mostrando a vulnerabilidade existente relacionada a sobrecargas. Esses testes possibilitaram analisar diversas ferramentas disponibilizadas pela AWS para tratar ataques DoS e DDoS.

Inicialmente foi observado que o servidor, sem nenhuma medida de proteção contra ataques ficava sobrecarregado e indisponível conforme o volume de tráfego de requisições aumentava. Com a implementação de medidas básicas de segurança, como a configuração de *firewalls* e a ativação de *SYN cookies* a instância servidor se mostrou mais resistente aos ataques, mantendo a disponibilidade em resposta às mesmas quantidades de requisições, ou seja, obteve

uma melhoria significativa em relação ao início. Mas apenas essas medidas não se mostraram 100% eficazes, conforme o gráfico 4 mostrou, houve um aumento brusco no tempo de resposta em um dado momento, o que indica que não há constância nessa técnica, conforme as instâncias atacantes e solicitações aumentarem, o tempo de resposta também aumentará.

Em seguida foram realizados os testes de ataques DDoS, para simular uma *botnet* foram criadas múltiplas instâncias atacantes, novamente sem medidas de proteção pré configuradas o servidor atingiu o ponto de indisponibilidade em um dado momento. Para mitigar esse problema foram implementadas medidas de proteção avançadas, como grupos de segurança, balanceador de carga e as ferramentas AWS WAF & Shield, assegurando uma proteção ainda mais robusta e mantendo o servidor disponível e estável mesmo diante de ataques em larga escala, assegurando a disponibilidade do servidor mitigando o tipo de ataque DDoS volumétrico.

3.5.1 Sobre os Custos

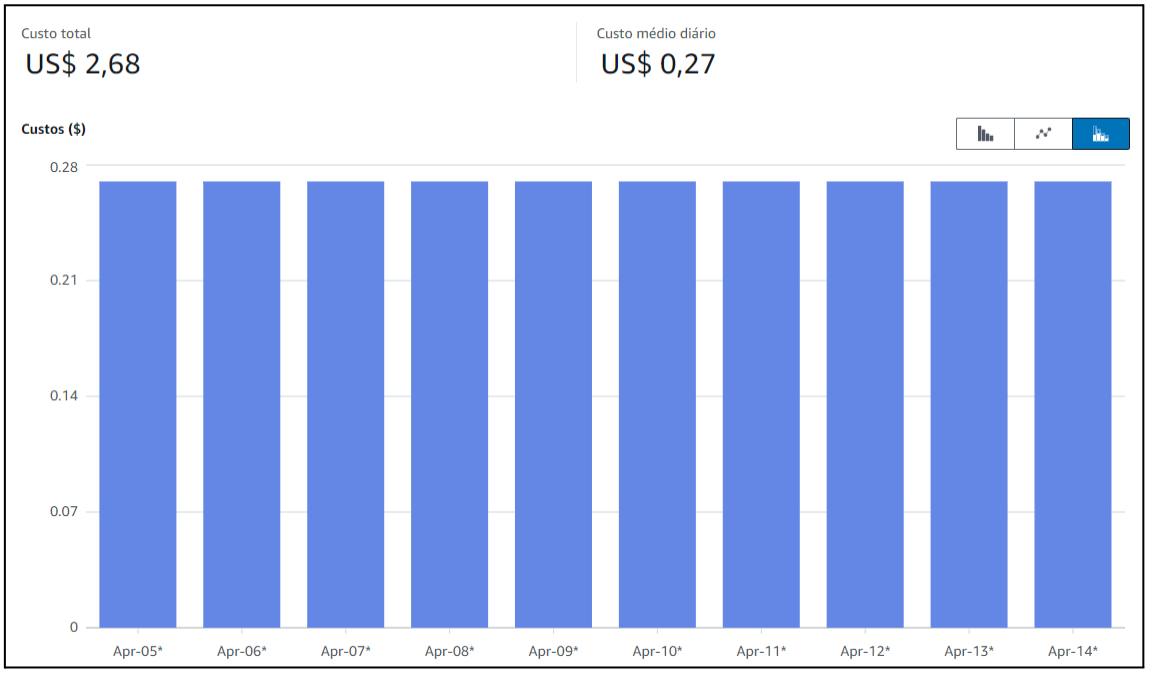
Apesar dos custos em relação ao servidor terem aumentado, devido a implementação de métodos de segurança contra ataques DDoS, os benefícios resultantes dessas medidas de proteção são inegáveis. A análise detalhada revelou que, ao adotar medidas eficientes para identificar e mitigar os ataques de negação de serviço distribuídos, as organizações podem evitar tanto danos diretos aos seus sistemas, quanto os prejuízos financeiros que viriam decorrentes de indisponibilidade nos serviços

Ao comparar os resultados dos testes realizados nos ambientes simulados, fica evidente que os métodos de segurança como o AWS WAF & Shield e balanceadores de carga desempenharam um papel fundamental na detecção e na mitigação das ameaças. Os custos relacionados a implementação dessas soluções, individualmente, deixam evidente que é possível garantir a segurança e disponibilidade de uma aplicação por valores relativamente pequenos para o cliente, conforme mostram os gráficos 13 (WAF & Shield) e 14 (Application Load Balancing).

Além disso, quando se avalia o custo-benefício dos métodos de segurança, é importante considerar os potenciais custos de uma possível interrupção do serviço devido a um ataque DDoS, embora inicialmente as técnicas de segurança adicionais

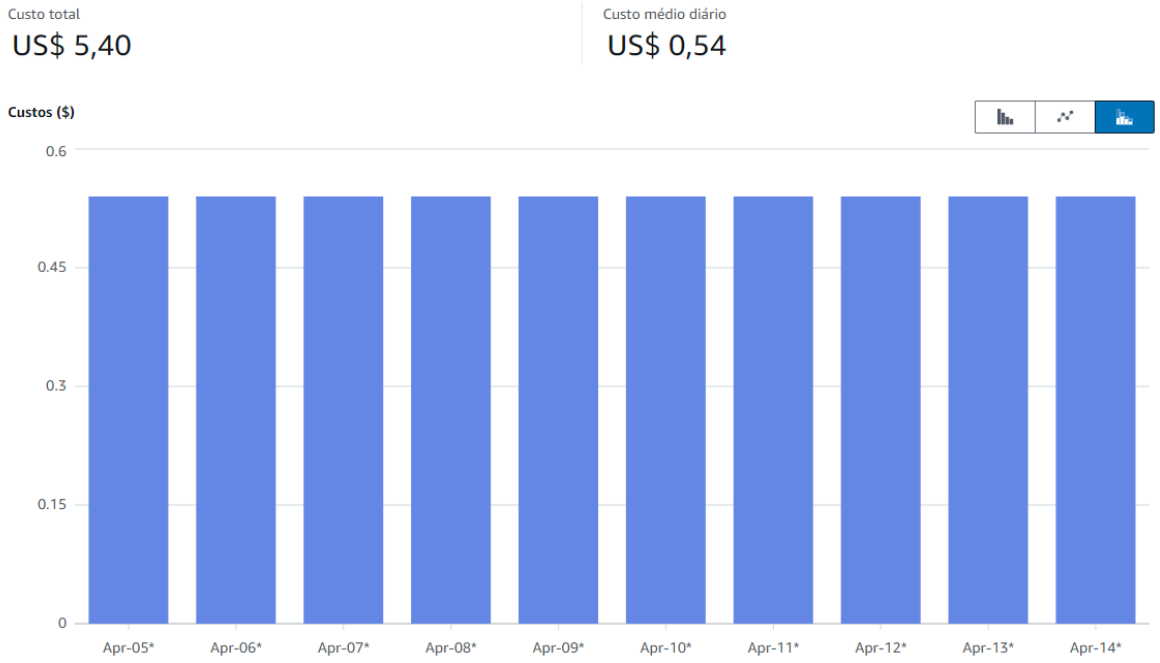
possam representar um investimento inicial levemente mais elevado, esse custo é totalmente justificado pela redução do risco de perdas financeiras e reputacionais que poderiam acontecer mediante a indisponibilidade do sistema.

Gráfico 13 - Análise dos Custos Relacionados ao Serviço WAF & Shield



Fonte: Gerado automaticamente pelo AWS Cost Explorer (2023).

Gráfico 14 - Análise dos Custos Relacionados ao Application Load Balancing



Fonte: Gerado automaticamente pelo AWS Cost Explorer (2023).

4. DISCUSSÃO DO TRABALHO

O principal objetivo deste estudo foi entender como os ataques de negação de serviço distribuídos (DDoS) são formados e usados para atacar computadores em nuvem pública. Além disso, foram analisados quais são os custos e benefícios de diferentes estratégias para se proteger contra esses ataques, investigar as ferramentas disponíveis para essa proteção, realizar testes para ver o quão bem essas ferramentas funcionam e analisar as soluções de segurança oferecidas pela AWS. Durante o estudo, foram obtidos diversos resultados, como:

A. Custos e Impactos Econômicos: Analisando os custos relacionados à implementação de medidas de segurança, destaca-se a importância de se considerar diversos fatores relacionados à indisponibilidade de um serviço, como os investimentos em sistemas de segurança e também os possíveis impactos econômicos que podem causar. Isso ressalta a necessidade de um planejamento cuidadoso na análise de riscos e valor dos ativos de informação.
B. Ferramentas de Proteção: Ao investigar uma variedade de ferramentas de proteção disponíveis para lidar com uma *botnet* usada em um ataque DDoS, foi possível mostrar a diversidade de abordagens e tecnologias disponíveis para mitigar esse tipo de ataque, dentre elas, cita-se o trabalho conjunto entre o *firewall* do kernel do sistema operacional, AWS WAF & Shield, *security group*, *application load balancing* e *auto scaling group*.
C. Testes de Desempenho: A realização de testes em um ambiente controlado permitiu avaliar o desempenho das ferramentas de proteção selecionadas contra ataques DDoS, esses testes forneceram *insights* sobre a eficácia e a capacidade de resposta das ferramentas em cenários reais.
D. Análise das Soluções da AWS: Investigar e analisar as soluções de segurança oferecidas pela AWS proporcionou uma compreensão mais aprofundada das ferramentas disponíveis e como usá-las para proteger infraestruturas de nuvem contra ataques DDoS.

Durante a análise dos resultados, foi possível identificar alguns padrões e tendências relacionados à eficácia das ferramentas de proteção em diferentes cenários de ataque. Observamos também diferenças nas respostas das ferramentas

testadas, destacando a importância de uma abordagem flexível na defesa contra ataques DDoS.

5. RECOMENDAÇÕES FUTURAS E CONCLUSÕES

Para ampliar ainda mais as possibilidades de futuras pesquisas, além das que já foram exploradas no trabalho, é interessante considerar outras abordagens para reforçar a segurança e resiliência das infraestruturas em nuvem contra ataques distribuídos de negação de serviço e ameaças cibernéticas.

Seria benéfico investigar alternativas às ferramentas tradicionais de proteção contra *botnets* em ataques DDoS em vez de se concentrar exclusivamente em soluções convencionais, explorar abordagens baseadas em inteligência artificial e aprendizado de máquina pode proporcionar uma defesa mais adaptável contra ameaças cibernéticas em constante evolução.

Em relação aos testes de desempenho das ferramentas de proteção, seria útil considerar a realização de testes práticos em ambientes de produção controlados. Isso garantiria uma avaliação mais precisa da eficácia das ferramentas em condições reais de operação.

Por fim, explorar soluções oferecidas por outros provedores de serviços em nuvem pode proporcionar uma visão mais abrangente das opções disponíveis. Isso incluiria a análise comparativa de ferramentas de proteção de terceiros e a consideração de soluções de código aberto e de comunidade como alternativas viáveis. Essas abordagens podem contribuir significativamente para o avanço do conhecimento no campo da segurança em nuvem e para a melhoria da resiliência das infraestruturas em nuvem contra ameaças cibernéticas.

O presente trabalho proporcionou um estudo sobre a investigação de como as *botnets* são utilizadas em ataques de negação de serviço distribuídos contra infraestruturas de nuvem pública de computadores. Durante o desenvolvimento do projeto, foram investigadas as técnicas de infecção de dispositivos para torná-los *bots* de uma rede e as estratégias empregadas por essas redes de dispositivos comprometidos para sobrecarregar serviços em nuvem e torná-los indisponíveis. Além disso, compreendemos a eficácia de uma variedade de medidas de proteção e mitigação buscando entender como as organizações podem se defender de ataques DDoS.

Os resultados alcançados vão além de gráficos estatísticos, mas *insights* que podem ajudar na construção de estratégias de segurança, tornando-se dados importantes para garantir que as infraestruturas de nuvem pública permaneçam protegidas, confiáveis e disponíveis em frente aos desafios contínuos da segurança da informação.

REFERÊNCIAS

FOROUZAN, B. A. Comunicação de Dados e Redes de Computadores. Porto Alegre: AMGH Editora, 2013.

LEVESON, N. G. Computer-Related Risks. Addison-Wesley, 1995.

CAMARGO, Carla O. et al. Avaliação sobre a qualidade de conjuntos de dados associados a ataques de negação de serviço . *In*: **SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO (SBSI)**, 14. , 2018, Caxias do Sul. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2018. p. 358-365.

HEINRICH, Tiago. et al. Um Estudo de Correlação de Ataques DRDoS com Fatores Externos Visando Dados de Honeypots. *In*: **SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG)**, 22. , 2022, Santa Maria. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2022. p. 358-371. DOI: https://doi.org/10.5753/sbseg.2022.225328.

HEINRICH, T. and Obelheiro, R. R. Brasil vs Mundo: Uma análise comparativa de ataques DDoS por reflexão. *In:* **Anais do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais**, São Paulo, SP, Brasil. SBC, 2019.

LEMMI, Tarina. Saiba o que é computação em nuvem e como funciona. Acesso em: abril 03, 2024. Disponível em: https://vexpenses.com.br/blog/computacao-nuvem/, 2023.

NUNES, Everson. Botnet: conheça essa ameaça digital e saiba como se proteger". Acesso em: abril 03, 2024. Disponível em: https://vnx.partners/o-que-e-botnet-e-como-se-proteger/, 2022.

E. Bertino and N. Islam. Botnets and internet of things security, *in:* **Computer**, v. 50, no. 2, p. 76-79, Feb. 2017, doi: 10.1109/MC.2017.62.

N. Hoque, D. K. Bhattacharyya and J. K. Kalita. Botnet in DDoS attacks: trends and challenges, *in:* **IEEE Communications Surveys & Tutorials**, v. 17, n. 4, p. 2242-2270, Fourthquarter 2015, doi: 10.1109/COMST.2015.2457491.

M. Bailey, E. Cooke, F. Jahanian, Y. Xu and M. Karir. A survey of botnet technology and defenses. **Cybersecurity Applications & Technology Conference for Homeland Security**, Washington, DC, USA, 2009, pp. 299-304, doi: 10.1109/CATCH.2009.40.

O que é segurança da nuvem?. **Microsoft**. Acesso em: 12 de abril de 2024. https://www.microsoft.com/pt-br/security/business/security-101/what-is-cloud-security

O que é uma botnet?. **Keeper**. Acesso em 12 de abril de 2024, from https://www.keepersecurity.com/blog/pt-br/2024/01/18/what-is-a-botnet/, 2024.

GOMES, Marcelo R. A formação de profissional de TI no âmbito da segurança da informação: estudo de caso em Instituições de ensino superior de Santa Catarina. Florianópolis: IFSC, 2017.

Amazon Web Services. What is AWS WAF?. Acesso em: abril 03, 2024. Disponivel em: docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

Amazon Web Services. AWS Managed Rules for AWS WAF – IP Reputation. Acesso em: abril 03, 2024. Disponivel em: https://docs.aws.amazon.com/waf/latest/developerguide/aws-managed-rule-groups-ip-rep.html

BRANQUINHO, Thiago; Marcelo. Segurança Cibernética Industrial. Editora Alta Books, 2021. E-book. ISBN 9786555204117. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555204117/. Acesso em: 12 abr. 2024.

BARRO, Vitória. Segurança na nuvem: melhores práticas e como implementá-las. **Hostinger Tutoriais**. acesso em 13 de abril de 2024. Disponível em: https://www.hostinger.com.br/tutoriais/seguranca-na-nuvem, 2023

Guerra Cibernética e os conflitos na era da Informação. Compugraf. https://www.compugraf.com.br/blog/guerra-cibernetica/, 2020.

Informática, S. Principais vantagens da escalabilidade em nuvem para empresas. **Safetec**. Acesso em: 10 de abril de 2024. Disponível em: https://safetec.com.br/cloud-computing/escalabilidade-nuvem/#:~:text=A%20escalabilidade%20na%20nuvem%20%C3%A9%20a%20capacidade%20de%20ampliar%20os,de%20158%20milh%C3%B5es%20de%20assinantes, 2023.

ALVES, David; PEIXOTO, Mario; ROSA, Thiago. Internet das coisas (IoT): segurança e privacidade de dados pessoais. Editora Alta Books, 2021. E-book. ISBN 9786555202793. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555202793/. Acesso em: 12 abr. 2024.

EREMIN, Alexander. What are botnets downloading?. **Kaspersky**, 2018. Disponível em: https://securelist.com/what-are-botnets-downloading/87658/. Acesso em: 09 abr. 2024.

FERREIRA, Arthur E. G.; NOGUEIRA, Michele. Identificando botnets geradoras de ataques DDoS volumétricos por processamento de sinais em grafos. *In*: **WORKSHOP DE GERÊNCIA E OPERAÇÃO DE REDES E SERVIÇOS (WGRS)**, 2018, Campos do Jordão. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2018 . ISSN 2595-2722.

LEÔNCIO, Pedro F. de Melo. CAMPOS, Maria R. Sampaio. Avaliação de escalabilidade e desempenho de um sistema de arquivos distribuído oportunista para redes locais. Acesso em: 11 de abril de 2024, Disponível em: http://splab.ufcg.edu.br/~joaopedro/finalreport.pdf, 2012.

Cloud Computing: o que é e como funciona?. **Salesforce**. Acesso em 12 de abril de 2024. Disponível em: https://www.salesforce.com/br/cloud-computing/#:~:text=De%20uma%20forma%20simples%2C%20cloud,qualquer%20computador%2C%20em%20qualquer%20lugar.

Admin, U. O que é alta disponibilidade em nuvem?. **Blog Saphir.** Acesso em 13 de abril de 2024. Disponível em: https://blog.saphir.com.br/o-que-e-alta-disponibilidade-em-nuvem/, 2023.

PIRES, Luiza. O que é botnet? Conheça o controle remoto dos cibercriminosos. **Welivesecurity**. Acesso em 13 de abril de 2024, from https://www.welivesecurity.com/pt/conscientizacao/o-que-e-botnet-conheca-o-controle-remoto-dos-cibercriminosos/, 2024.

Yaltirakli, Gokberk. Slowloris. Recuperado de https://github.com/gkbrk/slowloris, 2015.

SCHLEMER, Eligio. Iptables protege contra SYN FLOOD? Acesso: 31 de março de 2024. Disponível em: https://www.vivaolinux.com.br/artigo/Iptables-protege-contra-SYN-FLOOD, 2007.

SILVA, Cayo Valsamis, ALVES, Gabriel de C. Eiras, FERNANDES, Lucas S de Brito. (2016). O modelo cliente servidor. Acesso em: março 31, 2024. Disponível em: https://www.gta.ufrj.br/ensino/eel878/redes1-2016-1/16_1/p2p/modelo.html

CERF, V.; KAHN, R. A protocol for packet network intercommunication. *In* **IEEE Transactions on Communications**, v. 22, n. 5, p. 637-648, maio 1974, doi: 10.1109/TCOM.1974.1092259.

CIS. Ensure tcp syn cookies is enabled. **Tenable**. Acesso em: 26 de abril de 2024. Disponível em: https://www.tenable.com/audits/items/CIS_Distribution_Independent_Linux_Server_L1_v2.0.0.audit:abc9e627b9d021e79b9b61d854f6ba0d, 2024.